



(12) 发明专利申请

(10) 申请公布号 CN 101765996 A

(43) 申请公布日 2010. 06. 30

(21) 申请号 200880100663. 3

(74) 专利代理机构 北京集佳知识产权代理有限

(22) 申请日 2008. 05. 30

公司 11227

(30) 优先权数据

代理人 朱胜 陈炜

11/756,088 2007. 05. 31 US

(51) Int. Cl.

H04L 9/00 (2006. 01)

(85) PCT申请进入国家阶段日

2010. 01. 27

(86) PCT申请的申请数据

PCT/US2008/065216 2008. 05. 30

(87) PCT申请的公布数据

W02009/025905 EN 2009. 02. 26

(71) 申请人 威斯科数据安全国际有限公司

地址 瑞士苏黎士 - 弗卢加芬

(72) 发明人 弗兰克·库利耶 弗兰克·霍尔内特

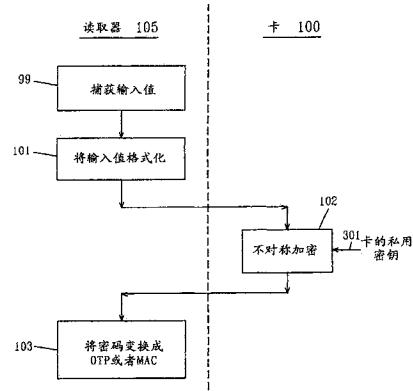
权利要求书 7 页 说明书 19 页 附图 12 页

(54) 发明名称

远程认证和交易签名

(57) 摘要

本发明提供一种允许使用包含PKI私用密钥的设备（比如具有PKI功能的智能卡或者USB棒）来认证用户并且对交易进行签名的方法、装置、计算机可读介质和信号。用户和/或消息的真实性被检验。进而，进行操作（认证和/或签名）而无需应用程序与包含私用密钥的设备具有某种直接或者间接的数字连接。换而言之，并不要求数字连接，所述数字连接允许应用程序将数据提交到卡以便由卡的私用密钥签名，并且允许从卡取回整个所得签名。此外，进行操作而无需包含私用密钥的具有PKI功能的设备（例如PKI智能卡或者USB棒）支持对称密码运算，或者已经用可以由适当读取器读取的某种保密或者机密数据元来私人化。



1. 一种用于生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的方法, 包括 :

获得使用一个或者多个可变输入和运用至少一个秘密的密码算法来创建的中间动态值 ;

将所述动态值转换成所述安全值,

其中执行利用私用密钥的不对称密码运算以产生密码, 以便变换所述动态值, 并且所述变换包括产生大小比所述不对称密码运算生成的密码的大小更小的所述安全值。

2. 根据权利要求 1 所述的方法, 其中所述一个或者多个可变输入包括以下值中的一个或者多个值 :

时间值 ;

计数器值 ;

挑战值 ;

交易数据 ; 或者

前述值的任何组合。

3. 根据权利要求 2 所述的方法, 其中创建所述中间动态值包括使用以下数据中的一个或者多个数据 :

对生成所述安全值的设备进行标识的数据 ; 或者

存储于生成所述安全值的所述设备中的一个或者多个秘密 ; 或者

对生成所述安全值的设备的用户进行标识的数据 ; 或者

与所述私用密钥关联的数据 ; 或者

由生成所述安全值的设备的用户提供的秘密。

4. 根据权利要求 2 所述的方法, 其中 :

将所述动态值转换成所述安全值包括以下操作中的一个或者多个操作 :

散列 ;

用对称密码算法来加密或者解密 ;

截取 ;

选择某些位、半字节或者字节 ; 或者

十进制换算。

5. 根据权利要求 2 所述的方法, 还包括 :

使用第一设备来捕获所述一个或者多个可变输入的值并且呈现所述安全值,

使用第二设备来存储所述私用密钥并且执行所述不对称密码运算, 其中

所述第二设备从所述第一设备接收信息并且将信息发送到所述第一设备, 并且

所述第一设备将信息发送到所述第二设备并且从所述第二设备接收信息。

6. 根据权利要求 3 所述的方法, 还包括 :

使用第一设备来捕获所述一个或者多个可变输入的值并且呈现所述安全值,

使用第二设备来存储所述私用密钥并且执行所述不对称密码运算, 其中

所述第二设备从所述第一设备接收信息并且将信息发送到所述第一设备, 并且

所述第一设备将信息发送到所述第二设备并且从所述第二设备接收信息。

7. 根据权利要求 5 所述的方法, 其中 :

所述第一设备是具有键盘和显示器的由电池供电的智能卡读取器。

8. 根据权利要求 6 所述的方法, 其中 :

所述第一设备是具有键盘和显示器的由电池供电的智能卡读取器。

9. 根据权利要求 5 所述的方法, 其中 :

所述第二设备是智能卡。

10. 根据权利要求 5 所述的方法, 其中 :

所述第二设备是 USB 棒。

11. 根据权利要求 5 所述的方法, 其中 :

所述第一设备是 PC 或者 PDA 或者移动电话。

12. 根据权利要求 2 所述的方法, 其中 :

所述安全值取决于所述私用密钥的值。

13. 根据权利要求 12 所述的方法, 其中 :

所述安全值是所述不对称密码运算使用所述私用密钥生成的所述密码的值的函数。

14. 根据权利要求 13 所述的方法, 其中 :

根据所述一个或者多个可变输入中的至少一个可变输入计算的值用作向所述不对称密码运算的输入, 并且

所述中间动态值是所述不对称密码运算产生的所得密码的函数。

15. 根据权利要求 13 所述的方法, 其中 :

计算所述安全值包括使用对称密码算法, 其中

根据所述不对称密码运算使用所述私用密钥生成的所述密码来导出所述对称密码算法中所用的密钥。

16. 根据权利要求 5 所述的方法, 其中 :

所述第一设备将第一设备挑战提交到所述第二设备 ;

所述第二设备使用所述私用密钥对所述第一设备挑战执行不对称密码运算, 并且将所得密码返回到所述第一设备 ;

所述第一设备验证所述所得密码 ; 并且

所述第一设备在所述所得密码的所述验证成功的条件下生成所述安全值。

17. 根据权利要求 16 所述的方法, 其中 :

通过使用所述一个或者多个可变输入和对称密码运算的计算来获得所述中间动态值。

18. 根据权利要求 17 所述的方法, 其中 :

根据所述一个或者多个可变输入来导出用于所述对称密码运算的数据 ; 并且

根据所述对称密码运算的输出来导出所述中间动态值。

19. 根据权利要求 17 所述的方法, 其中 :

所述对称密码运算使用根据以下数据中的一个或者多个数据导出的对称秘密 :

标识所述第一设备的数据 ;

存储于所述第一设备中的一个或者多个秘密 ;

与所述私用密钥关联的数据 ;

存储于所述第二设备上的数据 ;

标识所述第一设备的用户的数据 ; 或者

所述第一设备的用户提供的秘密。

20. 根据权利要求 16 所述的方法，其中将第一设备挑战至少两次提交到所述第二设备，从而产生所述初始呈现的初始密码和第二次呈现的以后密码；并且所述方法还包括：

根据所述初始密码导出参考值；

在所述第一设备中存储所述参考值；并且

通过比较所述以后密码与存储的所述参考值来验证所述以后密码。

21. 根据权利要求 16 所述的方法，还包括：

维持将至少一个第一设备挑战与至少一个对应验证值一起存储于所述第一设备中；并且

其中所述所得密码的所述验证包括比较所述所得密码与所述对应验证值。

22. 根据权利要求 16 所述的方法，还包括：

在所述第一设备与所述第二设备一起初次使用期间执行包括以下操作的序列：

生成所述至少一个挑战；

将所述至少一个挑战提交到所述第二设备以便所述第二设备使用所述私用密钥执行不对称密码运算；

从所述第二设备接收至少一个所得密码；

根据所述至少一个所得密码导出验证值；并且

将所述至少一个挑战与所述至少一个验证值一起存储。

23. 根据权利要求 22 所述的方法，其中所述第一设备有时执行包括以下操作的序列：

生成新设备挑战；

将所述新设备挑战提交到所述第二设备，以便所述第二设备使用所述私用密钥执行不对称密码运算；

从所述第二设备接收对应新密码；

根据所述对应新密码导出新验证值；并且

在存储器中将所述新设备挑战与所述新验证值一起存储。

24. 根据权利要求 23 所述的方法，其中：

所述新设备挑战和所述新验证值替换更早的设备挑战和验证值。

25. 根据权利要求 24 所述的方法，其中每当所述验证成功时执行所述序列。

26. 根据权利要求 17 所述的方法，其中：

所述第一设备对所述所得密码进行的所述验证要求使用与所述第二设备的所述私用密钥对应的公共密钥。

27. 根据权利要求 26 所述的方法，其中：

所述第一设备验证与所述公共密钥对应的证书或者证书链。

28. 根据权利要求 27 所述的方法，其中：

所述第一设备在存储器中维护证书当局的公共密钥；并且

所述第一设备对所述证书或者证书链进行的所述验证要求使用所述证书当局的所述公共密钥。

29. 一种使用根据权利要求 2 所述的方法来生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的装置。

30. 根据权利要求 29 所述的装置,包括读取器,所述读取器用于 :
基于所述一个或者多个可变输入来生成用于所述不对称密码运算的输入,
将所述输入传达到所述不对称密码运算,并且
接收所述不对称密码运算的所得不对称密码,并且
根据所述所得密码导出所述中间动态值。

31. 根据权利要求 29 所述的装置,包括读取器,所述读取器用于 :
将输入传达到所述不对称密码运算,并且
接收所述不对称密码运算的所得不对称密码,并且
根据所述所得不对称密码导出对称密钥,并且
使用所述对称密钥与对称密码算法来计算所述安全值。

32. 根据权利要求 29 所述的装置,包括 :
读取器,用于 :
将读取器挑战传达到所述不对称密码运算,并且
接收所述不对称密码运算的所得不对称密码 ;并且所述装置还包括 :
存储器,用于存储参考值 ;并且所述装置还包括 :
处理单元,用于 :
通过比较所述所得不对称密码与存储的所述参考值来验证所述所得不对称密码,并且
在所述所得不对称密码的所述验证成功的条件下生成所述安全值。

33. 根据权利要求 29 所述的装置,包括 :
读取器,用于 :
将读取器挑战传达到所述不对称密码运算,并且
接收所述不对称密码运算的所得不对称密码 ;并且所述装置还包括 :
处理单元,用于 :
通过使用与所述私用密钥对应的公共密钥,并且通过验证与所述公共密钥对应的证书
或者证书链,来验证所述所得不对称密码 ;在所述所得不对称密码的所述验证成功的条件下
生成所述安全值。

34. 根据权利要求 33 所述的装置,还包括 :存储器,用于
存储证书当局的用来验证与所述公共密钥对应的所述证书或者证书链的公共密钥。

35. 根据权利要求 29、31 和 32 中的任一权利要求所述的装置,还包括电池电源、键盘和
显示器。

36. 根据权利要求 35 所述的装置,还包括执行所述不对称密码运算的智能卡。

37. 一种使用户提供的安全值生效以便认证所述用户或者与所述用户关联的数据的方法,所述安全值包括一次性口令或者包括消息认证代码的签名 ;所述方法包括 :

 使用参考密码算法来创建参考密码,所述参考密码算法使用服务器密钥来应用于一个
或者多个参考输入,所述服务器密钥是可信用户的 PKI 私用密钥的值的函数,所述参考密
码算法和所述一个或者多个参考输入被选择为与所述可信用户在创建所述安全值时使用
的对应要素相同 ;

 在这之后,

 通过将所述参考密码变换为参考安全值,单独对所述参考密码进行操作,包括产生大

小比所述参考密码的大小更小的所述参考安全值，并且实现所述参考安全值与所述安全值的比较，或者

对所述参考密码和所述安全值两者进行操作，以产生修改的参考密码和修改的安全值，并且实现修改的所述参考密码与修改的所述安全值的比较，并且

根据所述比较的结果确定所述安全值的有效性。

38. 根据权利要求 37 所述的方法，其中：

为了产生修改的所述参考密码而对所述参考密码进行的所述操作与为了创建所述安全值而执行的操作部分地相同。

39. 根据权利要求 37 所述的方法，其中所述参考密码算法是不对称算法，并且所述服务器密钥具有与所述可信用户的所述 PKI 私用密钥相同的值。

40. 根据权利要求 37 所述的方法，其中所述参考密码算法是对称算法，并且根据使用所述可信用户的 PKI 私用密钥生成的密码来导出所述服务器密钥。

41. 一种使用户提供的安全值生效以便认证所述用户或者与所述用户关联的数据的方法，所述安全值包括一次性口令或者包括消息认证代码的签名并且使用根据权利要求 1 所述的方法来生成，所述方法包括：

使用参考密码算法来创建参考密码，所述参考密码算法使用服务器密钥来应用于一个或者多个参考输入，所述服务器密钥和所述参考密码算法和所述一个或者多个参考输入被选择为与所述可信用户在创建所述安全值时使用的对应要素相同；

通过将所述参考密码转换成参考安全值，对所述参考密码进行操作，包括产生大小比所述不对称密码运算已经生成的所述密码的大小更小的所述参考安全值；并且

对所述安全值进行操作以产生修改的安全值；并且

实现所述参考安全值与修改的所述安全值的比较；并且

根据所述比较的结果确定所述安全值的有效性。

42. 根据权利要求 41 所述的方法，其中：

对所述参考密码进行的所述操作与为了创建所述安全值而执行的操作部分地相同。

43. 一种支持指令序列的计算机可读介质，所述指令在执行时实现一种生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的方法，所述方法包括：

获得使用一个或者多个可变输入和运用至少一个秘密的密码算法来创建的中间动态值；

将所述动态值转换成所述安全值，

其中执行利用私用密钥的不对称密码运算以产生密码，以便变换所述动态值，并且

所述变换包括产生大小比所述不对称密码运算生成的密码的大小更小的所述安全值。

44. 根据权利要求 43 所述的计算机可读介质，其中所述一个或者多个可变输入包括以下值中的一个或者多个值：

时间值；

计数器值；

挑战值；

交易数据；或者

前述值的任何组合。

45. 根据权利要求 44 所述的计算机可读介质, 其中创建所述中间动态值包括使用以下数据中的一个或者多个数据 :

对生成所述安全值的设备进行标识的数据 ; 或者
存储于生成所述安全值的设备中的一个或者多个秘密 ; 或者
对生成所述安全值的设备的用户进行标识的数据 ; 或者
与所述私用密钥关联的数据 ; 或者
由生成所述安全值的设备的用户提供的秘密。

46. 根据权利要求 44 所述的计算机可读介质, 其中 :

将所述动态值转换成所述安全值包括以下操作中的一个或者多个操作 :

散列 ;
用对称密码算法来加密或者解密 ;
截取 ;
选择某些位、半字节或者字节 ; 或者
十进制换算。

47. 一种包括指令序列的信息承载信号, 所述指令在处理器中执行时实现一种生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的方法, 所述方法包括 :

获得使用一个或者多个可变输入和运用至少一个秘密的密码算法来创建的中间动态值 ;

将所述动态值转换成所述安全值,
其中执行利用私用密钥的不对称密码运算以产生密码, 以便变换所述动态值, 并且
所述变换包括产生大小比所述不对称密码运算生成的密码的大小更小的所述安全值。

48. 根据权利要求 47 所述的信息承载信号, 其中所述一个或者多个可变输入包括以下值中的一个或者多个值 :

时间值 ;
计数器值 ;
挑战值 ;
交易数据 ; 或者
前述值的任何组合。

49. 根据权利要求 48 所述的信息承载信号, 其中创建所述中间动态值包括使用以下数据中的一个或者多个数据 :

对生成所述安全值的设备进行标识的数据 ; 或者
存储于生成所述安全值的设备中的一个或者多个秘密 ; 或者
对生成所述安全值的设备的用户进行标识的数据 ; 或者
与所述私用密钥关联的数据 ; 或者
由生成所述安全值的设备的用户提供的秘密。

50. 根据权利要求 48 所述的信息承载信号, 其中 :

将所述动态值转换成所述安全值包括以下操作中的一个或者多个操作 :

散列 ;
用对称密码算法来加密或者解密 ;

截取；
选择某些位、半字节或者字节；或者
十进制换算。

51. 一种认证多个用户的方法，其中各用户具有至少一个关联智能卡，所述智能卡包含至少一个PKI私用密钥，并且能够用所述PKI私用密钥执行不对称密码运算，所述方法包括以下步骤：

为与用户关联的各智能卡生成服务器侧密钥，并且
从所述用户接收包括OTP或者MAC的安全值，并且

使用所述服务器侧密钥根据权利要求41所述的方法通过使接收的所述安全值生效来认证所述用户。

52. 根据权利要求51所述的方法，包括以下步骤：

对于各用户，将挑战提交到与所述用户关联的所述智能卡，以便使用所述私用密钥对所述智能卡进行不对称密码运算；并且

从所述智能卡接收所述智能卡上的所得密码；并且

在生成所述服务器侧密钥时，在所述智能卡上通过所述私用密钥来使用所述所得密码。

53. 根据权利要求51所述的方法，包括以下步骤：

生成一个或者多个保密密钥导出种子；并且

在生成所述服务器侧密钥时，使用所述保密密钥导出种子中的至少一个保密密钥导出种子；并且

向所述用户送达在生成所述服务器侧密钥时使用的所述保密密钥导出种子中的所述至少一个保密密钥导出种子，用于与这些用户关联的所述智能卡。

54. 根据权利要求51所述的方法，包括以下步骤：

从存储于所述智能卡上的证书获得与各所述用户关联的数据；并且

在生成所述服务器侧密钥时使用来自所述证书的所述数据。

远程认证和交易签名

背景技术

[0001] 随着计算机系统和应用的远程访问日益普及,通过公共网络如因特网来远程访问的交易数目和种类已经急剧增加。这一普及已经特别地凸显对安全性的需要。

[0002] a. 如何确保远程访问应用的人士是他们所声称的人士以及如何确保远程进行的交易由合法个人发起。这一主题称为认证。

[0003] b. 如何确保交易数据在被应用服务器接收到之前未被更改。这称为数据完整性。

[0004] c. 如何保证个人一旦已经参与交易就不能够赖债。这称为认可。

[0005] 应用提供者以往一直依赖于静态口令来为远程应用提供安全性。在过去数年已经变得明显的是,静态口令是不足的,并且要求更高级的安全技术。

[0006] PKI 智能卡

[0007] 一种解决与通过公共网络对计算机系统和应用的远程访问关联的安全问题的方式由公共密钥基础结构提供。在公共密钥基础结构中,将公共 - 私用密钥对与各用户关联。密钥对与将该公共 - 私用密钥对绑定到特定用户的证书(由受信任的证书当局签发)关联。借助不对称密码术,这一公共 - 私用密钥对可以用来:

[0008] a. 认证用户,

[0009] b. 对交易、文档、电子邮件签名(以便防止赖债),以及

[0010] c. 建立加密的通信通道。

[0011] 为了保证足够水平的安全性,强制各用户的私用密钥保持保密并且仅能由与该密钥关联的合法用户访问(以例如创建签名)。普遍依赖于智能卡来存储公共 - 私用密钥对和证书,并且进行涉及到私用密钥的密码计算。通过卡来使用私用密钥于是常常受 PIN 保护。

[0012] 具有 PKI 功能的智能卡正在并且已经由:

[0013] a. 公司签发给它们的雇员或者客户,以保障对它们的计算机网络的登录或者对它们的应用的远程访问;

[0014] b. 银行签发给它们的客户,以保障例如网上银行应用;以及

[0015] c. 政府签发给它们的市民作为电子 ID 卡,以创建依法绑定的电子签名。

[0016] 除了优点之外,也存在一些与 PKI 以及携带 PKI 密钥和证书的智能卡关联的缺点:

[0017] a. 在与有竞争力的安全技术比较时,构建公共密钥基础结构一般很复杂并且因此成本高。

[0018] b. PKI 内在地限于其中在客户机与服务器之间有数字连接的环境和应用。换而言之,它并不适合于电话银行或者其它如下交付通道,在这些交付通道中,无法在一方面是 PKI 证书和私用密钥的容器与另一方面是应用服务器之间提供数字连接。

[0019] c. PKI 智能卡没有电源或者用户接口。PKI 智能卡因此依赖于对接设备的存在,该对接设备向卡提供电力,能够以数字方式与卡交换数据,并且能够与用户对接(例如捕获卡的 PIN 并且呈现应当签名的数据)。在大多数情况下,使用具有连接透明的智能卡读取器

的 PC。这减少了用户的灵活性（许多 PC 未配备智能卡读取器）。它也带来了安全问题：在内在不安全的 PC 上完成所有用户交互（比如批准签名或者捕获卡的 PIN）。

[0020] 强认证令牌

[0021] 一种用于认证和交易签名能力的可选技术由称为‘强认证令牌设备’的设备提供。强认证令牌的典型例子是由 Vasco Data Security 公司提供的任一数字通 (Digipass) 令牌，见网站 Vasco. com。

[0022] 强认证令牌是小型自治的由电池供电的设备，该设备具有它自己的显示器和键盘。在一些情况下，键盘简化为单个按钮或者甚至完全被省略。强认证令牌的主要目的在于生成所谓的“一次性口令”(OTP)。在一些情况下，强认证令牌也能够对在令牌的键盘上已经输入的数据生成电子签名或者消息认证代码 (MAC)。如果令牌具有键盘，则对令牌的使用常常由 PIN 保护。为了能够生成 OTP 或者 MAC，强认证令牌能够基于用保密值或者密钥参数化的对称密码算法来完成密码计算。用保密值或者密钥参数化的这样的对称密码算法的典型例子是对称加密 / 解密算法（比如 3DES 或者 AES）和 / 或密钥化 (keyed) 单向散列函数（比如符合 OATH 的令牌中的 MD5 或者 SHA-1）。在本文的其余部分中，这样的算法的输出有时会称为‘对称密码’。术语‘对称密码’因此应当不仅理解为对称加密算法的输出，而且理解为对称解密算法或者密钥化散列函数的输出。用假设为对于每个个别令牌而言不同的一个或者多个保密密钥将强认证令牌私人化。为了生成一次性口令或者签名，令牌通常执行以下步骤（参照图 1）：

[0023] a. 步骤 10：令牌取得某一输入值（这可以是由服务器生成的并且由用户在键盘上键入的挑战、和 / 或令牌的内部实时时钟的值、和 / 或由令牌管理的内部计数器的值、和 / 或由用户在键盘上键入的交易数据）。

[0024] b. 步骤 11：令牌将输入值表达成指定格式。

[0025] c. 步骤 12：令牌然后将这一格式化的输入提交到用安全地存储于令牌中的私人化保密密钥 15 参数化的对称加密 / 解密算法和 / 或单向散列函数。结果是密码或者散列值。

[0026] d. 步骤 13：令牌将作为这一加密 / 解密或者单向散列的结果的密码或者散列值变成实际的 OTP 或者 MAC，即密码或者散列通常被截取、以人类可读格式转换（例如通过十进制换算）以及在显示器上可视化。用户可以将这个值提交到应用服务器。

[0027] 在大多数情况下，强认证令牌是物理设备，然而在一些情况下，这些强认证令牌生成 OTP 或者 MAC 签名的功能由在 PC、工作站、移动电话、个人管理器、PDA 等上运行的软件模仿。后者称为“软令牌”。

[0028] 一旦已经产生 OTP 或者 MAC，就将它传达到实体，在所述实体处可以验证该值作为认证用户或者消息，参见图 2。该实体通常是应用服务器。应用服务器为各令牌存储数据，该数据包括已经用哪一个或者多个保密密钥将令牌私人化以及与令牌关联的用户的身份。为了使一次性口令或者签名生效，服务器收回保密密钥 (115)（它是令牌中私人化的密钥的副本），取得令牌所用的相同输入，并且进行本质上与令牌相同的算法 112。服务器然后比较 120 它获得的结果与它接收的值。（在实践中，如果强认证算法由于同步问题而基于时间或者基于计数器，则 OTP 或者 MAC 的生效常常有些更复杂。）由于强认证令牌生成的一次性口令或者签名是令牌的个别保密密钥和针对令牌算法的一个或者多个输入的总是

不同的值的函数,所以使一次性口令或者签名的正确性生效向应用服务器给予了下述很高置信度:提交一次性口令或者签名的个人拥有正确令牌并且知道它的 PIN(如果令牌受 PIN 保护),这又给予了下述高置信度:该个人确实是与该令牌设备关联的合法用户。

[0029] 由于 OTP 验证服务器和 OTP 令牌本质上用相同密钥进行相同算法,所以 OTP 生成算法可以是单向或者不可逆函数。这意味着实际 OTP 可以比用来导出它的密码或者散列值更短。这允许充分短的 OTP 或者 MAC 长度,从而用户将 OTP 或者 MAC 值从令牌显示器手工复制到 PC 上并非很不便。因而强认证令牌并不要求在令牌与认证服务器之间的数字连接。

[0030] 强认证令牌在与 PKI 卡比较时的主要优点在于:

[0031] a. 它们为全自治(令牌具有它们自己的电源和它们自己的用户接口);

[0032] b. 它们独立于交付通道或者通信介质(令牌并不要求与任何其它设备的任何数字或者电子连接;所有数据输入和输出由用户经由令牌的显示器和键盘来完成);以及

[0033] c. 它们提供很高水平的安全性(所有用户交互(比如捕获 PIN 或者提供待签名的交易数据)都经由令牌自己的安全用户接口来完成)。

[0034] 在其中已经签发智能卡的一些情况下,想要回避与智能卡关联的缺点和限制,并且实现强认证令牌提供的相同优点,即全自治、独立于交付通道和安全用户接口。

[0035] 一种可选方式是组合智能卡与未连接的由电池供电的智能卡读取器,该读取器具有它自己的显示器和键盘。想法是智能卡与未连接的智能卡读取器的组合模仿强认证令牌。强认证令牌通常提供的功能然后在智能卡与未连接的读取器上划分。未连接的读取器负责所有用户接口,而其它令牌功能的全部或者部分交给卡。

[0036] 通常,所有私人化的秘密和对安全性敏感的数据由卡存储和管理(例如 PIN 由卡存储和验证,保密密钥存储于卡上,而涉及到这些密钥的所有密码运算由卡完成,作为用于令牌算法的输入来使用的计数器由卡存储和管理)。令牌功能的敏感性较低的部分(例如截取和转换生成的散列或者密码)常常出现在读取器中。下文讨论这一组合的例子。

[0037] 这一原理常常由银行使用,这些银行组合它们签发的银行卡(用于在自动取款机或者销售点终端使用)与未连接的读取器,以保护它们的远程银行应用(比如网上银行或者电话银行)。这一点的适合例子是 Mastercard Chip Authentication Programme(CAP),该 CAP 指定 EMV 智能卡可以如何与未连接的智能卡读取器组合,以生成一次性口令和电子交易数据签名。

[0038] 这一技术依赖于智能卡能够完成对称密码运算,并且已经用保密密钥来私人化,以用于对称密码运算。然而,具有 PKI 功能的智能卡被设计成存储不对称密钥并且完成不对称密码运算。许多具有 PKI 功能的智能卡并不支持对称密码运算或者(如果它们支持则)从未用个别对称保密密钥来私人化。

[0039] 传统 PKI 签名

[0040] 用 PKI 智能卡创建电子签名的常用方式是输入数据(输入数据通常由想要签名的实际交易数据的散列构成)由卡的私用密钥加密。

[0041] 使这样的签名生效的常用方式是生效实体用公共密钥对接收的签名解密。如果签名的解密获得与假设已经由私用密钥加密的输入数据相同的值,则使签名成功生效。注意由于这一不对称特性,生效实体从不需要访问卡的私用密钥。这允许私用密钥向签名方以外的任一方、甚至向任何验证方保密,由此提供真正的认可。

[0042] 只有签名本身在整体上可为生效实体所用,才可以成功完成这一点。不完整签名的解密将仅获得不能与假设已经签名的输入数据比较的无意义数据。

[0043] 在实践中,当使用小型手持未连接的智能卡读取器时,不能满足这一条件:假如典型PKI签名大小为100字节数量级,那么这些读取器的显示器小到远远无法显示全部签名,并且在任何情况下期望用户将100字节的值从读取器的显示器手工传送到PC而不犯一个错误全然不切实际。100字节的典型PKI签名应当与传统强认证令牌的典型6到8数位或者3到4字节的OTP或者MAC比较。这的确是不对称密码术和私用密钥为何尚未用来例如通过强认证令牌生成OTP和MAC的原因。

[0044] 希望的是如下方法和装置,该方法和装置:

[0045] a) 允许将存储PKI私用密钥的设备(比如具有PKI功能的智能卡或者USB棒)用来认证用户并且对交易进行签名;

[0046] b) 如果没有必要,则无需任何用户应用与容纳私用密钥的设备具有某种直接或者间接数字连接、特别是如下数字连接,该数字连接将允许用户应用将数据提交到卡,以便由卡的私用密钥签名,并且将允许从卡收回整个所得签名,

[0047] c) 无需容纳私用密钥的具有PKI功能的设备(例如PKI智能卡或者USB棒):

[0048] 1) 支持对称密码运算;或者

[0049] 2) 已经用可以由适当读取器读取的一些保密或者机密数据元来私人化。

发明内容

[0050] 本申请提供对一种满足上述希望的方法和装置的描述。具体而言,本申请描述多个实施例,这些实施例使用公共-私用密钥对中的私用密钥(将用于不对称密码术例如RSA算法的密钥)来认证用户(经由OTP的生成)或者对数据签名(经由MAC的生成)。

[0051] 这里描述的实施例与传统上使用私用密钥来认证用户和对数据进行签名(如上所述)的不同之处在于:

[0052] a) 使用相同密码术密钥来生成和验证OTP和MAC;并且

[0053] b) OTP和MAC值的位长度可以安全地显著少于私用密钥生成的密码的位长度。

[0054] 所有实施例的共同之处在于:

[0055] a) 它们都借助密码算法使用一个或者多个可变输入来计算动态值,所述密码算法使用验证服务器也已知或者可访问的秘密。

[0056] b) 这些可变输入可以是以下输入中的任何输入:

[0057] 1) 时间值,或者

[0058] 2) 计数器值,或者

[0059] 3) 挑战值,或者

[0060] 4) 交易数据,或者

[0061] 5) 上述输入的任何组合。

[0062] c) 动态值然后被变换为OTP或者MAC。

[0063] d) 在开发OTP或者MAC的过程中的某一点,执行利用私用密钥的不对称密码运算(即加密或者解密或者签名)。

[0064] e) 将动态值变换为OTP或者MAC,使得OTP或者MAC的长度或者大小小于不对称

密码运算使用私用密钥生成的密码的大小。

[0065] 利用私用密钥的不对称密码运算在生成 OTP 或者 MAC 的整个处理中的确切作用可以随着实施例而不同。

[0066] 在一些实施例中,每当不得不生成 OTP 或者 MAC 时,进行利用私用密钥的不对称密码运算。在其它实施例中,可以与利用私用密钥的单个不对称密码运算结合生成多于一个的 OTP 或者 MAC。在后一种情况下,可以在需要生成新 OTP 或者 MAC 时对是否要求利用私用密钥的新不对称密码运算进行确定的标准可以包括:

[0067] a) 从上次不对称密码运算起已经过去的时间。

[0068] b) 已经生成的 OTP 和 / 或 MAC 的数目。

[0069] c) 在包含私用密钥的设备与捕获输入并且使 OTP 可用的设备之间的通信会话是否一直不间断(例如是否尚未从智能卡读取器移开 PKI 智能卡)。

[0070] d) OTP 或者 MAC 的类型。例如, MAC 的生成可能总是要求新的不对称密码运算,但是 OTP 的生成不会要求。

[0071] 在一个典型实施例中,使用仅一个私用密钥,并且用该私用密钥进行仅一个不对称密码运算。然而,一些实施例可以用单个私用密钥或者用多个私用密钥进行多个密码运算。例如:

[0072] a) 如果 OTP 是私用密钥对可变输入进行的加密结果的函数,则变体可以是:OTP 是多于一个的密码的函数,或者可变输入由多于一个的私用密钥加密以生成 OTP。

[0073] b) 如果 OTP 的生成仅在通过检查卡的私用密钥对挑战进行的加密结果来验证特定智能卡的存在之后发生,则变体可以是:将多于一个的挑战提交到卡以由卡的私用密钥加密。

[0074] c) 在许多情况下,PKI 卡包含所谓实用私用密钥和签名私用密钥。在该情况下,如果生成 OTP 则可以使用实用密钥,而如果生成 MAC 则可以使用签名密钥。

[0075] 在一个优选实施例中,可以生成用于认证用户的 OTP 和用于对数据签名的 MAC。然而,替代实施例可以限于仅能够生成 OTP 或者仅能够生成 MAC 签名。

[0076] 在一个典型实施例中,与私用密钥一起使用的不对称密码算法将是 RSA 算法。然而,其它实施例可以使用其它不对称算法,只要它们能够通过使用私用密钥来实现加密或者解密或者签名功能。这样的算法的例子包括:RSA、渐缩算法(比如 Merkle-Hellman 或者 Chor-Rivest、Pohlig-Hellman、Diffie-Hellman、ElGamal、Schnorr、Rabin)、椭圆曲线密码系统、有限自动机公共密钥密码系统、数字签名算法(DAS、DSS)。

[0077] 在一个典型实施例中,包含私用密钥的部件以及生成 OTP 和 MAC 值的部件是两个不同部件,各部件是两个不同设备的部分。然而,可以容易地设想如下实施例,在这些实施例中,这两个部件是相同设备的部分或者甚至是相同部件。

[0078] 在一个典型实施例中,私用密钥存储于智能卡上。在一个优选实施例中,涉及到私用密钥的密码计算由该智能卡进行。在一个典型实施例中,OTP 和 / 或 MAC 值由如下设备生成,该设备配备有或者连接到可以与包含私用密钥的智能卡通信的部件或者设备。

[0079] 在一个优选实施例中,卡读取设备是未连接的智能卡读取器,该读取器具有它自己的电源,并且运行适当软件以与已经插入智能卡读取器中的 PKI 智能卡通信,以生成 OTP 或者 MAC。

[0080] 在另一实施例中，卡读取设备是一些计算设备如 PC、PDA、蜂窝电话等的组合，这些计算设备配备有智能卡读取器，并且运行适当软件以生成 OTP 或者 MAC。

[0081] 在一个典型实施例中，在智能卡与智能卡读取器设备之间的通信的电性和协议方面与 ISO 7816 标准中描述的方面相同或者相似。其它实施例可以使用其它通信装置，比如 ISO 14443 中描述的无接触智能卡。

[0082] 可选的形式因素可用于私用密钥包含设备，并且可选的形式因素可用于 OTP 或者 MAC 生成设备，而且可选的装置可用于在一方面是私用密钥包含部件或者设备与另一方面是 OTP 和 MAC 生成部件或者设备之间的通信。这些可选的因素和装置处在如这里描述的本发明的范围内。

[0083] 在一个实施例中，OTP 或者 MAC 值可视化于卡读取设备的显示器上。OTP 可以例如由连串符号构成。在一个典型实施例中，这些符号是十进制数位。在其它实施例中，这些符号可以例如包括：

[0084] a) 十六进制数位，或者

[0085] b) 基本 64 数位，或者

[0086] c) 来自书写系统如字母表的字符，或者

[0087] d) 象形文字。

[0088] 在一个实施例中，生成的 OTP 或者 MAC 借助可听信号送达到用户。例如，OTP 可以是数位或者字符或者字词的串，各数位或者字符或者字词具有特性关联音调或者由文字到语音的转换器读取。

[0089] 在一个实施例中，生成的 OTP 或者 MAC 借助某种电子有线或者无线通信机制直接送达到应用程序。这一机制可以包括 USB 连接或者红外线连接或者近场通信连接或者 RF 连接或者蓝牙连接。

[0090] 可以提供用于 OTP 或者 MAC 的其它输出机制。在一些实施例中，基于私用密钥的函数受 PIN 保护。

[0091] 以下说明更具体地描述了基本实施例。在一些实施例中，在生成 OTP 或者 MAC 时直接或者间接使用卡的基于私用密钥的函数。

[0092] a) 涉及到卡的私用密钥的不对称密码运算是将可变输入变换成 OTP 或者 MAC（以对称方式使用不对称算法）的这一变换的整体阶段或者部分，或者

[0093] b) 卡的基于私用密钥的函数更间接用来提供种子值，该种子值用来导出 OTP 或者 MAC 生成算法所用的保密对称密钥（使用不对称密码作为种子以导出保密密钥）。

[0094] 在一些实施例中，OTP 和 / 或 MAC 的值是卡的私用密钥的实际值的函数。在更多其它实施例中，卡的基于私用密钥的函数用来将读取器中的 OTP 或者 MAC 生成算法解锁：

[0095] a) 卡链接到已经私人化的读取器，并且基于存储的一个或者多个挑战 - 响应对来进行识别，或者

[0096] b) 卡通过传统的基于 PK 证书的验证由读取器认证。

[0097] 在紧接在前段落中描述的实施例中，生成的 OTP 和 / 或 MAC 的值不是卡的私用密钥的实际值的函数。

[0098] 因此在一个方面中，本发明提供一种用于生成包括一次性口令 (OTP) 或者消息认证代码签名 (MAC) 的安全值的方法，该方法包括：

[0099] 获得使用一个或者多个可变输入和运用至少一个秘密的密码算法来创建的中间动态值；

[0100] 将所述动态值变换成所述安全值，

[0101] 其中，执行利用私用密钥的不对称密码运算以产生密码，以便变换所述动态值，并且

[0102] 所述变换包括产生大小比所述不对称密码运算生成的密码的大小更小的所述安全值。

[0103] 在另一方面中，本发明提供一种使用紧接上文描述的方法来生成包括一次性口令(OTP)或者消息认证代码签名(MAC)的安全值的设备。

[0104] 在另一方面中，本发明提供一种使用户提供的安全值生效以便认证用户或者与用户关联的数据的方法，所述安全值包括一次性口令或者消息认证代码签名；所述方法包括：

[0105] 使用参考密码算法来创建参考密码，该参考密码算法使用与可信用户的PKI私用密钥有关的服务器密钥来应用于一个或者多个参考输入，该参考密码算法和一个或者多个参考输入被选择为与可信用户在创建安全值时所用的对应要素相同；

[0106] 在这之后，

[0107] 通过将所述参考密码变换成参考安全值，单独对所述参考密码进行操作，包括产生大小比参考密码的大小更小的所述参考安全值，并且实现所述参考安全值与所述安全值的比较，或者

[0108] 对所述参考密码和所述安全值两者进行操作，以产生修改的参考密码和修改的安全值，对所述参考密码进行的所述操作与为了创建所述安全值而执行的操作部分地相同，并且实现修改的所述参考密码与修改的所述安全值的比较，并且

[0109] 根据所述比较的结果确定所述安全值的有效性。

[0110] 在又一方面中，本发明包括一种支持指令序列的计算机可读介质，这些指令在执行时实现一种生成包括一次性口令(OTP)或者消息认证代码签名(MAC)的安全值的方法，所述方法包括：

[0111] 获得使用一个或者多个可变输入和运用至少一个秘密的密码算法来创建的中间动态值；

[0112] 将所述动态值变换成所述安全值，

[0113] 其中执行利用私用密钥的不对称密码运算以产生密码，以便变换所述动态值，并且

[0114] 所述变换包括产生大小比所述不对称密码运算生成的密码的大小更小的所述安全值。

[0115] 最后在又一方面中，本发明包括一种指令序列的信息承载信号，这些指令在处理器中执行时实现一种生成包括一次性口令(OTP)或者消息认证代码签名(MAC)的安全值的方法，所述方法包括：

[0116] 获得使用一个或者多个可变输入和运用至少一个秘密的密码算法来创建的中间动态值；

[0117] 将所述动态值变换成所述安全值，

- [0118] 其中执行利用私用密钥的不对称密码运算以产生密码,以便变换所述动态值,并且
[0119] 所述变换包括产生大小比所述不对称密码运算生成的密码的大小更小的所述安
全值。

附图说明

- [0120] 现在在说明书的与以下附图结合时的后文部分中进一步描述本发明的若干实施例 :
- [0121] 图 1 是现有技术的强认证令牌在生成 MAC 的 OTP 时的操作流程图 ;
- [0122] 图 2 是现有技术的服务器在认证由强认证令牌生成的 OTP 或者 MAC 时的操作及其与 OTP 或者 MAC 生成的关系的流程图 ;
- [0123] 图 3 是依赖于使用 PKI 私用密钥来创建从中生成 OTP 或者 MAC 的密码的不对称密
码运算的本发明一个实施例的流程图 ;
- [0124] 图 4 是示出了在客户机的 OTP/MAC 生成 (例如如图 3 中那样) 和在服务器的有关
认证的本发明一个实施例的流程图 ;
- [0125] 图 5 是使用不对称密码作为种子以导出在创建代表 OTP 或者 MAC 的密码时所用密
钥的本发明另一个实施例的流程图 ;
- [0126] 图 6 和图 7 是其中智能卡用来向读取器认证用户的本发明又一实施例的流程图,
该读取器又产生从中导出 OTP 或者 MAC 的密码,在这一实施例中,在初始操作中将用户的智
能卡绑定到读取器 (图 6),而在图 7 中表示了随后的操作 ;
- [0127] 图 8 和图 9 是其中包括 PKI 证书的智能卡用来向读取器认证用户的本发明又一实
施例的流程图,该读取器又产生从中导出 OTP 或者 MAC 的密码,在这一实施例中可以认证随
机用户 ;
- [0128] 图 10 和图 11 图示了为了捕获允许本发明各种实施例操作的信息而在初始会话中
进行的动作 ;
- [0129] 图 12 图示了本发明实施例的操作背景 ;
- [0130] 图 13 是第一生效过程的图示 ;并且
- [0131] 图 14 是另一生效过程的图示。

具体实施方式

- [0132] 本发明实施例的重要部件在图 12 中被图示为包括智能卡读取器 20 (或者简称为
读取器) 和认证服务器 30 (或者简称为服务器)。
- [0133] 读取器 20 至少包括接口 28 以接受智能卡和电源 27。一些读取器也包括在图 12
中由键盘 25 代表的一个或者多个用户可操作按钮或者键。如这里使用的那样,用户将智能
卡插入智能卡接口 28 中。由于读取器 20 进行的某一操作,信息由读取器生成。该信息可以
是一次性口令 (OTP)。如果交易数据输入到读取器,则生成的信息可以包括签名,比如 MAC。
输出信息可以呈现于显示器如显示器 26 上。代替地,读取器可以用数字方式连接到网络。
在该情况下,信息可以呈现给也连接到网络的另一实体,而显示器 26 可能是不必要的。通常,
读取器 20 生成的信息用来认证个人或者消息。可以通过使用智能卡 (证明拥有该卡)

和一些其它信息（比如 PIN 或者其它用户数据）来认证个人。读取器接受智能卡和其它信息并且创建 OTP。OTP 送达到服务器 30。代替地，消息由读取器 20 签名从而产生 MAC，而该 MAC 送达到服务器 30。

[0134] 服务器 30 通常被实施为具有处理能力和数据库 35 的计算机。读取器生成的信息经由数据路径 40 送达到服务器 30。数据路径 40 可以采用各种形式。通常，用户将信息从显示器 26 手工传送到连接至服务器 30 的客户机设备。代替地，数据路径 40 可以包括允许信息从读取器 20 送达到服务器 30 的数字路径。作为另一可选方式，数据路径可以运送音频信息，比如运送如下用户的语音的电话电路，该用户念出在显示器 26 上向用户呈现的信息；其中该信息可以是 OTP 或者 MAC。数据路径 40 可以运送代表在读取器 20 生成的信息的光学信号。一般而言，数据路径 40 是可以用来将信息从读取器 20 送达到服务器 30 的任何路径。服务器 30 接受 OTP 或者 MAC，并且借助数据库 35 中的数据来确定是接受还是拒绝该信息作为使用户的身份 (OTP) 或者消息的可信性 (MAC) 生效。下文更具体地描述服务器 30 所用的具体过程和数据。服务器 30 的一个输出端选择接受或者拒绝状态 36，从而反映接受 OTP 作为使用户的声明的可信性生效，或者反映使 MAC 生效作为认证关联消息。

[0135] 以对称方式使用不对称算法

[0136] 在这一实施例（见图 3）中，智能卡 100 与智能卡读取器 105 配合。智能卡 100 存储在不对称密码运算中使用的 PKI 私用密钥 301。卡的基于私用密钥的函数（即涉及到卡的私用密钥的不对称密码运算，比如签名或者解密）是产生 OTP 或者 MAC 的过程的整体阶段或者部分。

[0137] OTP 和 / 或 MAC 的生成以如下方式发生：

[0138] 步骤 99 :捕获将在以后步骤中所用的输入值。

[0139] 步骤 101 :用于 OTP 或者 MAC 生成算法的一个或者多个输入被变换或者格式化成初始值。

[0140] 步骤 102 :初始值由卡的私用密钥 301 签名或者加密 / 解密。

[0141] 步骤 103 :将所得密码变换为 OTP 或者 MAC。

[0142] 在图 3 的例子中，OTP 或者 MAC 仅为不对称密码运算的结果的函数。然而在其它实施例中，OTP 或者 MAC 也可以是包括如下值的其它数据元的函数，这些值是可变输入的函数，但不是私用密钥 301 的函数。

[0143] 在一个典型实施例中，向 OTP 或者 MAC 生成算法的一个或者多个输入与用于传统强认证令牌中所用的一个或者多个强认证算法的输入相同或者相似。换而言之，这些输入可以选择为：

[0144] 时间值，或者

[0145] 挑战（通常由服务器提供），或者

[0146] 计数器值，或者

[0147] 交易数据，或者

[0148] 上述输入的任何组合。

[0149] 在一些实施例中，向 OTP/MAC 生成算法的一个或者多个附加输入或者参数可以包括：

[0150] 标识服务的数据（例如读取器序列号），或者

- [0151] 存储于设备中的秘密,或者
- [0152] 用户标识数据,或者
- [0153] 用户提供的保密代码或者保密值。
- [0154] 为了将这些一个或者多个输入格式化成初始值,步骤 101 可以比如包括以下操作:
 - [0155] 并置,或者
 - [0156] 散列,或者
 - [0157] 利用对称密码算法(例如使用设备中存储的或者用户提供的保密密钥)的加密 / 解密。
- [0158] 为了将所得密码变换成最终 OTP 或者 MAC 值,步骤 103 可以包括以下操作:
 - [0159] 散列(可能是使用读取器 105 中存储的或者用户提供的保密密钥的密钥化散列),或者
 - [0160] 利用对称密码算法(例如使用读取器 105 中存储的或者用户提供的保密密钥)的加密 / 解密,或者
 - [0161] 截取,或者
 - [0162] 选择某些位、半字节或者字节,或者
 - [0163] 十进制换算。后者可以实现如下:
 - [0164] 将待十进制转换的位串解释为数的大型二进制代表,或者按位组划分待十进制转换的位串,并且将各位组映射到十进制数位。典型例子是将位串划分成半字节,并且根据以下规则将各半字节映射到十进制数位。如果半字节的十六进制值为 0x0 到 0x9,则取得具有相同值的十进制数位;如果半字节的十六进制值为 0xA 到 0xF,则减去常数(在 0x6 与 0xA 之间),然后取得值与相减的结果相同的十进制数位,或者
 - [0165] 本领域技术人员已知的许多其它十进制换算算法。
- [0166] 现在描述生效阶段。在这一实施例中,生效服务器具有用来生成 OTP 或者 MAC 值的私用密钥 301 的副本,并且使用它来进行与用于生成 OTP 或者 MAC 值的算法本质上相同的算法。生效服务器:
- [0167] (参照图 4) 以某种方式获得或者重构或者猜测在生成 OTP 或者 MAC 时作为向 OTP 或者 MAC 生成算法的一个或者多个输入来使用的数据元的一个或者多个值;
- [0168] 在时间值的情况下,生效服务器可以具有它自己的与用于生成 OTP 或者 MAC 的时钟同步的时钟,
- [0169] 在挑战的情况下,挑战可以已经由生效服务器本身生成,或者可以已经由应用与接收的 OTP 或者 MAC 一起传递到生效服务器,
- [0170] 在计数器的情况下,生效服务器可以维护它自己的与用于生成 OTP 或者 MAC 的计数器值同步的计数器值,
- [0171] 在交易数据的情况下,这些数据可以已经由应用与接收的 OTP 或者 MAC 一起传递到生效服务器;
- [0172] 将用于 OTP 或者 MAC 生成算法的一个或者多个输入变换成初始值。
- [0173] 随后使用由生效服务器保持的私用密钥 301 的副本对初始值签名或者加密 / 解密(402)。生效服务器然后比较(403)所得参考密码与接收的 OTP 或者 MAC 值。如果所得参

考密码与接收的 OTP 或者 MAC 值匹配，则使签名成功生效。可以用多种方式完成这一比较：

[0174] 生效服务器在一些实施例中可以将参考密码变换为参考 OTP 或者 MAC 值，并且比较参考 OTP 或者 MAC 值与接收的 OTP 或者 MAC 值（例如通过检验它们是否相同），或者

[0175] 生效服务器可以根据接收的 OTP 或者 MAC 值来重构由私用密钥生成的原密码的部分，并且比较这一部分密码与参考密码的一个或者多个对应部分，或者

[0176] 生效服务器可以将参考密码变换为第一中间生效值，并且将接收的 OTP 或者 MAC 变换为第二中间生效值，并且比较第一和第二中间生效值。

[0177] 以下例子可以说明这一点（见图 14）。在这一例子中，基于如下密码来产生 OTP 或者 MAC，该密码是使用私用密钥 1308 的不对称加密的结果。服务器产生如下参考密码，该参考密码也是使用如下密钥 1324 的不对称加密的结果，该密钥是私用密钥 1308 的副本。如图 14 中所示：

[0178] - 读取器 1350 通过以下操作根据所述原密码来计算 OTP 或者 MAC：

[0179] ○选择所述所得密码的每个字节的每个第一位（1355），并且

[0180] ○将选择的所述位并置成位串（1356），并且

[0181] ○将所述位串解释为数的二进制说明，并且通过取得所述数的十进制代表来获得 OTP 或者 MAC（1357）

[0182] - 生效服务器使这一 OTP 或者 MAC 生效如下：

[0183] ○服务器通过将每个字节的除了每个第一位之外的所有位设置成 1 来修改参考密码（1364），并且

[0184] ○服务器将接收的 OTP 或者 MAC 解释为数的十进制代表，并且通过取得该数的二进制代表来获得位串（1359），并且

[0185] ○服务器通过将所述位串的每一位替换成如下字节来扩展所述位串（1360），该字节由附加以七个 1 位来扩展的该位构成，并且

[0186] ○服务器比较扩展的所述位串与修改的所述参考密码（1365）。

[0187] 这一过程的参数（选择每个字节的一位）为举例。本领域技术人员将能够选择适当参数以适合他们的需要和背景。具体而言，典型 RSA 密码约为 100 字节。选择各字节的一位将产生 100 位。这在每十进制数位约为 3 位时将产生用于 OTP 或者 MAC 的约 30 个十进制数位，这比 300 个十进制数位更实用，但是仍然可能被认为难以使用。在该情况下可以选择每 40 位中的一位，从而共计 20 位或者约 6 个十进制数位。也可以在使用对称密钥而不是不对称密钥的情况下，使用用于根据密码来生成 OTP 或者 MAC（通过选择密码的一些但是并非所有位来变换）的相同过程。典型对称密码包括约 100 位。在这一情况下，选择每八位之一将带来约 12 位或者 4 个十进制数位。这可能被认为是太小以至于无法免受攻击的数目。为了避免这一问题，仅使用每 4 位之一（而不是每 8 位之一）以带来约 25 位或者约 8 个十进制数位。

[0188] 在图 13 中图示了一种替代生效过程。图 13 的过程在产生客户机侧的密码（操作 1305）和服务器侧的参考密码（操作 1323）方面与图 14 的过程相同。如图 13 中所示：

[0189] 密码通过首先是变换 A（1306）、然后是变换 B（1307）这两个变换的序列来变换为 OTP 或者 MAC

[0190] 生效服务器使参考密码受到操作 1325 以产生修改的参考密码，操作 1325 与变换

A 的操作相同，

[0191] 生效服务器也使 OTP 或者 MAC 受到操作 (1327)，该操作是用于产生修改的 OTP 或者 MAC 的变换 B 的逆变换，

[0192] 生效取决于修改的 OTP 或者 MAC 与修改的参考密码的比较 (1328)。

[0193] 如针对图 14 的生效过程的情况那样，无论是用对称还是不对称密钥产生密码都可以使用图 13 的技术。

[0194] 与传统 PKI 签名验证对照，图 3 的方法并不要求全签名可为服务器所用（如结合图 13 或者 14 示范的那样）。即使除了私用密钥之外未使用附加保密代码或者密钥（由用户提供或者存储于设备中），该解决方案仍然可以提供很高水平的安全性。

[0195] 然而，只有生效服务器在它不得不使 OTP 或者 MAC 生效时具有卡的私用密钥的副本，才可以使用图 3 的技术。PKI 的全部要点确切地在于为了保障真正的认可，私用密钥决不可以被与该密钥关联的用户之外的任何人所用。在许多情况下，通过卡在不可能从卡提取私用密钥的情况下生成机载私用和公共密钥对来保障这一点。在其它情况下，密钥对在外部生成，然后注入卡中，但是过程然后将正常保证卡私人化系统中的私用密钥在注入卡中之后立即被破坏，并且不允许私用密钥的副本存在于卡外。换而言之，这一方法在许多情况下不会是适合的解决方案。

[0196] 使用不对称密码作为种子以导出保密密钥（图 5）

[0197] 在以下实施例中并不要求生效服务器在生效时访问私用密钥的副本。在这一实施例中，以与传统强认证令牌相同的方式生成 OTP/MAC。这一算法的所有步骤（捕获输入、将输入格式化、对格式化的输入进行加密或者散列、将所得密码或者散列变换成 OTP/MAC）由读取器 505 进行。在这一实施例中，本发明与常规实践不同之处在于读取器 505 如何获得对称保密强认证密钥。为了获得这一保密对称认证密钥，读取器 505 依赖于涉及到卡的私用密钥 520 的对卡 500 的操作。这一方法的一个基本实施例的主要步骤如下：

[0198] 1. 如果需要（即卡通过 PIN 保护私用密钥的使用），则读取器要求用户输入 PIN 并且将该 PIN 提交到卡。

[0199] 2. 假设卡 500 接受 PIN，未连接的卡读取器将固定值提交到卡以由私用密钥签名。这一固定值也称为‘读取器到卡的挑战’。

[0200] 3. 卡用它的私用密钥对给定挑战签名并且将所得密码返回到读取器。这一所得密码也称为‘卡到读取器的签名声响应’。

[0201] 4. 读取器使用所得密码作为种子以导出对称保密密钥。这一密钥也称为‘导出的强认证保密密钥’。

[0202] 读取器用导出的强认证保密密钥将强认证算法（完全由读取器进行）动态地私人化。换而言之，读取器使用导出的强认证保密密钥来执行强认证令牌算法。

[0203] 图 5 图示了一个适当实施例，该实施例示出了读取器 505 与卡 500 的交互。该处理可以要求用户输入 PIN 510 以便将卡 500 解锁。这一步骤是可选的，但是如果进行该步骤，则用户在 510 输入的 PIN 被送达 511 到待测试的卡 500。卡接受或者拒绝 PIN。测试卡 500 的响应 (512)，并且只有接受处理才继续。随后函数 513 捕获来自读取器、用户或者卡中的一些或者全部的输入值。函数 514 可以将一些或者所有输入值格式化。这些值中的一些或者所有值或者其它值可以形成向卡 500 发送（函数 515）的读取器到卡的挑战 515a。卡

500 通过用卡的私用密钥 520 进行密码运算来使用挑战 515a。卡到读取器的签响应 516a 这一所得密码被回送到读取器（函数 516）。响应 516a 然后用作种子以经由函数 517 创建保密值或者密钥 517a。密钥 517a 称为导出的保密强认证密钥。密钥 517a 然后在函数 518 处与函数 514 提供的格式化的值一起使用于密码运算中。最后在函数 519 处变换所得的密码以产生 OTP 或者 MAC。

- [0204] ‘读取器到卡的挑战’ 515a 可以是任何以下值：
 - [0205] 1. 对于某个批次的所有读取器而言相同的固定值。
 - [0206] 2. 对于给定读取器而言固定、但是对于各读取器而言具有不同值的固定值。
 - [0207] 3. 对于给定用户而言恒定、但是对于不同用户而言可以不同并且用户在读取器中输入至少一次的固定值。在实践中很有可能的是，每当使用卡时将输入这一值，或者仅在首次与某一读取器一起使用时将输入这一值，并且读取器然后将记住这一值。
 - [0208] 4. 存储于卡上可以由读取器读取的静态数据（例如公共密钥和证书或者卡序列号）
 - [0209] 5. 任何上述值的组合。
 - [0210] 6. 根据任何上述值导出的值。该导出可选地包括使用某一读取器秘密。
- [0211] 用于根据‘卡到读取器的签响应’来导出强认证保密密钥的算法可以利用以下技术（以及其他技术）：
 - [0212] 1. 提取一些数据元的位
 - [0213] 2. 并置一些数据源的一些部分
 - [0214] 3. 对称加密 / 解密算法（例如 DES、AES、...）
 - [0215] 4. 散列算法（例如 SHA-1）
- [0216] 用于根据‘卡到读取器的签响应’ 516a 来导出强认证保密密钥 517a 的算法除了‘卡到读取器的签响应’ 516a 之外还可以利用以下额外数据元：
 - [0217] 1. 对于某个批次的所有读取器而言相同的固定值。
 - [0218] 2. 对于给定读取器而言固定、但是对于各读取器而言具有不同值的固定值。
 - [0219] 3. 对于给定用户而言恒定、但是对于不同用户而言可以不同并且用户在读取器中输入至少一次的固定值。
 - [0220] 4. 存储于卡上可以由读取器读取的静态数据（例如与私用密钥关联的数据，比如公共密钥和证书或者卡序列号）。
 - [0221] 5. 任何上述值的组合。
- [0222] 这一描述仅提及对智能卡的单个私用密钥的使用和与该密钥关联的单个操作；如果卡包含多个一个的私用密钥，则读取器可以将‘读取器到卡的挑战’ 515a 提交到这些卡私用密钥中的各私用密钥，并且在导出‘导出的强认证保密密钥’ 517a 时组合所得的‘卡到读取器的签响应’ 516a。
- [0223] 类似地，读取器也可以将不同的‘读取器到卡的挑战’ 值 515a 提交到卡，并且在导出‘导出的强认证保密密钥’ 517a 时组合所得的‘卡到读取器的签响应’ 516a。
- [0224] 在又一实施例中，读取器并不依赖于单个‘读取器到卡的挑战’ 515a 以及对应的‘卡到读取器的签响应’ 516a 和‘导出的强认证保密密钥’ 517a，而代之以使用一组‘读取器到卡的挑战’ 515a 以及对应的‘卡到读取器的签响应’ 516a 和‘导出的强认证保密密钥’ 517a。

钥’ 517a。为了获得‘导出的强认证保密密钥’ 577a, 读取器选择这些‘读取器到卡的 515a 挑战’之一并且将它提交到卡。选择哪个‘读取器到卡的挑战’ 515a 确定了对应的‘卡到读取器的签名声应’ 516a 和‘导出的强认证保密密钥’ 517a。这一选择因此必须以对于生效服务器而言可预测的方式发生。读取器可以例如按固定顺序遍历这组‘读取器到卡的挑战’ 515a, 或者可以取决于对强认证令牌算法的一个或者多个输入的值来选择‘读取器到卡的挑战’ 515a。后一种方法的简单例子是强认证令牌算法在挑战 - 响应模式中工作, 并且挑战的一个特定数位(例如末位)表明待使用的‘读取器到卡的挑战’的索引。

[0225] 由于私用密钥对于各卡而言不同, 所以导出的保密密钥对于给定挑战而言将为给定卡所特有。换而言之, 在读取器中的强认证算法中使用的保密密钥是卡(或者更精确地为该卡中的私用密钥 520)的函数。这意味着原则上需要访问正确的卡以能够生成正确的OTP。

[0226] 在大多数情况下, 私用密钥受 PIN 保护, 从而除了访问正确的卡之外也需要知道卡的 PIN 以能够生成正确的 OTP。

[0227] 如果读取器向卡提交的用于由私用密钥签名的固定值对于不同读取器而言可以不同, 则除了其它要素(例如访问正确的卡和知道卡的 PIN)之外也需要正确的读取器。注意: 对于不同读取器而言不同的值的这样的使用将读取器有效地‘绑定’到卡。

[0228] 为了生效服务器能够使以这一方式生成的强认证 OTP 和 / 或 MAC 生效, 它必须知道导出的强认证保密密钥 517a 的值。服务器因此必须知道卡的签名声应 516a。用于给定的卡挑战的卡签名声应由卡的私用密钥 520 确定, 并且在没有访问私用密钥 520 的情况下不能加以计算。这样做的一个后果是, 服务器必须访问卡的私用密钥 520(直接或者间接)至少一次。

[0229] 如果在卡上内部生成密钥对, 则这意味着服务器需要访问卡至少一次, 从而服务器可以向卡提交将适用于这一用户的一个或者多个卡挑战, 并且取回和存储对该一个或者多个挑战的一个或者多个卡响应(间接访问私用密钥)。如果密钥对在外部生成、然后注入卡中, 则服务器可以直接使用私用密钥, 以在卡外的私用密钥被破坏之前对一个或者多个挑战加密。

[0230] 服务器这时才能够根据加密的卡挑战来计算对应导出的强认证密钥。这一点的缺点在于, 在实践中, 用户将不得不在一种注册阶段期间向服务器授予对他 / 她的卡的访问权, 或者(在外部密钥生成的情况下)必须允许服务器在该私用密钥值被破坏之前用私用密钥值对挑战加密。

[0231] 另一后果是, 在实践中对于某一用户而言, 导出的强认证保密密钥必须保持不变。由于根据对某一卡挑战的卡的签名声应而对导出的强认证保密密钥进行导出, 所以该卡挑战和对应的‘卡到读取器的签名声应’对于给定用户而言必须保持固定。这一点的缺点在于, 如果攻击者获得某个用户的‘卡到读取器的签名声应’的值, 则该攻击者可能潜在地伪造如下卡, 这些卡在插入读取器中时总是返回该记录的“卡到读取器的签名声应”。

[0232] 在生成‘读取器到卡的挑战’和 / 或根据‘卡到读取器的签名声应’来导出‘导出的强认证保密密钥’时包括读取器特有或者用户特有的数据元, 可以使攻击者更难以获得正确的‘卡到读取器的签名声应’或者将该值与读取器一起用来以欺诈方式生成正确的 OTP 或者 MAC。

[0233] 使攻击者更难以获得正确的‘卡到读取器的签名声应’的另一方式如上文说明的那样，并不依赖于单个‘读取器到卡的挑战’以及对应的‘卡到读取器的签名声应’和‘导出的强认证保密密钥’，而代之以使用一组‘读取器到卡的挑战’以及对应的‘卡到读取器的签名声应’和‘导出的强认证保密密钥’。

[0234] 在以下实施例中，完全不要求服务器访问卡至少一次以进行私用密钥操作。

[0235] 在这一实施例中，对称保密认证密钥的值并不（直接或者间接）取决于卡的私用密钥的值。并未借助涉及到卡的私用密钥的不对称密码运算根据由卡生成的种子来导出对称保密认证密钥。代之以用对称保密认证密钥或者用读取器可以从中动态地导出对称保密认证密钥的保密数据将读取器私人化。利用这一对称保密认证密钥，读取器可以生成恰如传统强认证令牌一样的OTP或者MAC。对读取器的使用受保护，并且通过将用户的卡逻辑地绑定到读取器来为合法用户而保留。一旦用户的卡已经绑定到读取器，那么只有用户插入绑定到读取器的卡，读取器才会生成OTP或者MAC。卡因此起到访问密钥的作用以将私人化的读取器解锁。

[0236] 在首次使用时，读取器将请求插入用户的卡。在插入卡时，读取器以如下方式将本身逻辑地绑定到插入的卡。读取器确定和记住该卡的一些特有个别特性。这些特性可以包括：

[0237] ○卡序列号

[0238] ○卡的公共密钥和 / 或证书

[0239] ○对给定挑战的卡的响应（其中将响应定义为卡的私用密钥对挑战的加密；注意：这将通常要求用户提交PIN以将私用密钥解锁）。这一挑战和对应的卡的响应必须由读取器记住。挑战可以是：

[0240] ■固定总挑战（对于所有卡和所有读取器而言相同）

[0241] ■每读取器的固定挑战

[0242] ■每卡的固定挑战（例如在首次呈现卡时由读取器随机生成、然后由读取器记住）

[0243] ■用户提供的挑战

[0244] ■任何上述挑战的组合

[0245] 在图6中图示了这一操作的例子。读取器600等待接收卡数据（函数616）。卡将一些卡数据611提供给读取器（函数610）。当读取器接收到卡数据611时存储数据（函数617）。

[0246] 如果用户想要生成动态口令或者签名（见图7），则读取器询问绑定到该读取器的卡。读取器检验呈现的卡是否确实为期望的卡。即它将取回呈现的卡的特性（函数710），并且比较它们与绑定到读取器的卡的存储特性（函数711）。这一步骤可以包括：

[0247] ■读取卡的序列号

[0248] ■读取卡的公共密钥和 / 或证书

[0249] ■将（存储的）挑战提交到卡，以便由卡的私用密钥加密（可以要求用户提供PIN以将私用密钥解锁），并且接收卡的响应。

[0250] 在呈现的卡成功生效时，读取器继续执行如普通强认证令牌那样的强认证算法。

[0251] 为了加强安全性，许多变化是可能的。读取器可以根据以下各项来导出对称保密

认证密钥：

- [0252] ○在读取器中预先私人化的数据元
- [0253] ○和 / 或用户向读取器提供的数据元
- [0254] ○和 / 或读取器从卡读取的数据元
- [0255] 优选地，这些数据元是保密的。代替总是使用在卡绑定到读取器时使用和获得的相同挑战和对应的卡响应，读取器可以使用多对挑战和对应的响应。按照这一原理的变化包括：
 - [0256] ○当卡绑定到读取器时，读取器生成和提交多于一个的挑战到卡并且记住对应的卡响应。当读取器以后需要使卡生效时，它可以将这些挑战的任何子集提交到卡，并且检验卡的响应是否与存储的响应匹配。
 - [0257] ○当读取器已经使插入的卡成功生效时，它可以生成新挑战并且从卡获得对应的响应。这一新挑战 - 响应对然后可以由读取器记住，作为先前已知的一个或者多个挑战 - 响应对的替代或者附加对。
 - [0258] ○可以组合这两种变化。
- [0259] 又一实施例（图 8 和图 9）的原理如下。代表服务器，基于对用户的 PKI 卡的认证，读取器借助传统证书在本地认证用户。
- [0260] 如果用户由读取器成功认证，则读取器生成可以由生效服务器生效的 OTP 或者 MAC（使用传统强认证令牌算法）。用户然后可以将这一 OTP 或者 MAC 提交到服务器作为他已经由读取器成功认证的证据。
- [0261] 读取器借助用户的插入的 PKI 卡并且使用传统 PKI 技术来本地认证用户。在一个典型实施例中这可以完成如下（参照图 8）：
 - [0262] 1. 读取器 800 使卡的证书（或者证书链）806 生效。
 - [0263] a. 注意：这假设读取器具有对（根）证书当局的受信任公共密钥的访问权。这可以通过在读取器中存储（根）证书当局的受信任公共密钥来完成。
 - [0264] b. 注意：读取器 800 无需每当在读取器中插入卡时都完成从（根）CA 公共密钥开始对整个证书（链）的显式验证。代替地，读取器 800 可以在卡 805 首次插入读取器中时完成整个验证。读取器然后可以存储验证的证书和证书的公共密钥或者根据验证的证书或者公共密钥导出的参考值（例如证书或者公共密钥的散列）。如果然后在以后时间插入卡 805，则读取器 800 不再需要完成与证书生效关联的所有计算，而是可以仅比较卡上的证书与存储于读取器中的证书或者参考值。
 - [0265] 2. 读取器 800 进行卡的私用密钥的挑战 - 响应认证：
 - [0266] a. 读取器（810）生成挑战 811，例如通常为随机数或者某一其它非可预测的值，其例如使用读取器中存储的某一秘密借助密码算法根据时间值或者计数器值而导出。
 - [0267] b. 用户提供保护卡的私用密钥的 PIN。
 - [0268] c. 读取器 800 将 PIN 提交到卡。
 - [0269] d. 读取器 800 将随机挑战 811 提交到卡以由卡的私用密钥加密。
 - [0270] e. 卡用它的私用密钥对读取器签名（815）并且返回响应（= 加密的挑战 816）。
 - [0271] f. 读取器 800 用卡的公共密钥（来自证书）对卡的响应进行解密。
 - [0272] g. 读取器比较 820 解密的卡响应与原来生成的挑战。如果解密的卡响应与原来生

成的挑战相同，则卡的私用密钥被认证，并且因此用户被认证。

[0273] 本质上，读取器以与传统强认证算法相同的方式生成 (825) OTP/MAC。这一算法的所有步骤（捕获输入、将输入格式化、对格式化的输入进行加密或者散列、将所得密码或者散列转换成 OTP/MAC）以与传统强认证令牌本质上相同的方式由读取器 800 完成。在一个实施例中，用对称保密强认证密钥将读取器私人化。在该情况下，读取器 800 也通常被配置成期望特定的卡。读取器借助卡的数据元的某一特性值来识别该卡。通常，卡的证书用作这样的数据元。在其它实施例（见图 9）中，为了避免不得不对读取器进行私人化和配置，读取器 800 根据以下数据元来为对称保密强认证密钥导出 (835) 卡特有的值：

[0274] ○优先地与卡的证书或者公共密钥有关的公共卡数据（例如卡序列号、证书序列号、公共密钥等）

[0275] ○存储于读取器中并且为服务器所知的主密钥 846。这一主密钥可以是：

[0276] ■用于所有读取器的相同值

[0277] ■用于各个别读取器的特定 / 唯一值。这要求读取器向用户的某种分配和这一分配在服务器的注册。

[0278] ○（可选）额外导出数据元可以是用户向读取器提供的（保密）数据元。用户必须显式地提供这一数据元：

[0279] ■每当以这一方式使用读取器和卡时，或者

[0280] ■仅当这一卡首次与这一读取器一起使用时（此后读取器将记住提供的用于这一卡的数据元的值）

[0281] 读取器 800 在对称强认证算法（比如数字通算法或者 OATH）中使用导出的卡特有的对称认证密钥 836，以生成 (845) 动态口令（基于挑战 - 响应和 / 或时间和 / 或事件），或者生成 (845) 对一些交易数据（可选地包括时间和 / 或事件计数器信息）的 MAC 型电子签名。

[0282] 服务器使生成的动态口令或者签名生效如下：

[0283] ■服务器导出与读取器相同的卡特有的对称强认证密钥。这假设服务器具有将用户链接到以下数据的数据库（或者取回所需信息的替代方式）：

[0284] ○公共卡数据，

[0285] ○用户提供的数据元（如果适用）

[0286] ○以及读取器的主密钥

[0287] 注意：代替每当必须完成生效时完成这一导出，也可以一次完成导出，并且所得的导出密钥可以存储于数据库中以供将来使用。

[0288] ■服务器以与它针对传统强认证令牌而完成的方式相同的方式使动态口令或者签名生效。

[0289] 一个典型的实施例操作如下（图 10-11）：

[0290] 在招募阶段中，银行客户 1001 前往银行支行 1003。客户将他的全国电子身份证卡 (e-id 卡 1002) 与银行支行终端 (BBT) 一起用来对电子银行合同 1004 进行电子签名。

[0291] 在客户的 e-id 卡插入 BBT 中时 (1010)，BBT：

[0292] ○捕获客户的证书 (1011)，

[0293] ○生成随机种子挑战 (1012)，

- [0294] ○将随机种子挑战提交到 e-id 卡 (1002) 以由卡的私用密钥加密 (1013)，
- [0295] ○捕获该挑战上的卡密码 (1014)。
- [0296] 最后，BBT 将客户的证书、生成的种子挑战和种子挑战上的卡密码发送到服务器 (1015)。服务器将这一数据存储于链接到客户的数据仓库中。银行然后将未连接的智能卡读取器交付给客户。这一读取器包含保密主密钥。银行也向客户发送 PIN 邮包，该 PIN 邮包具有 BBT 生成和使用的种子挑战的值。也向认证服务器通知保密主密钥的值。
- [0297] 当客户首次使用读取器时：
- [0298] ○读取器要求插入客户的 e-id 卡。
- [0299] ○读取器也询问 PIN 邮包的种子挑战并且将它存储于存储器中。
- [0300] ○读取器读取卡的证书并且将它也存储于存储器中。
- [0301] ○读取器生成随机读取器挑战，并且将它提交到卡，以由卡的私用密钥加密。读取器存储读取器挑战和由卡生成的对应密码。
- [0302] 如果客户想要生成 OTP (或者 MAC 或者响应或者 ...)，则读取器经过以下步骤：
- [0303] ○读取器要求插入客户的 e-id 卡。
- [0304] ○读取器使卡生效：
- [0305] ■读取器读取卡的证书并且比较它与存储的证书。
- [0306] ■如果检查成功，则读取器将存储的读取器挑战提交到卡进行签名，并且比较卡的密码与存储的密码。
- [0307] ○如果读取器已经使卡成功生效，则读取器生成保密认证密钥：
- [0308] ■读取器将存储的 PIN 邮包种子挑战提交到卡以便由卡加密。
- [0309] ■读取器现在根据以下各项来导出保密认证密钥：
- [0310] ■读取器中的保密主密钥，
- [0311] ■PIN 邮包种子挑战，
- [0312] ■该 PIN 的邮包种子挑战上的卡密码，
- [0313] ■卡的证书。
- [0314] ○读取器现在在强认证算法中使用生成的保密认证密钥（例如生成 OTP 或者 MAC）。
- [0315] 认证服务器能够验证所得的 OTP (或者 MAC)，因为它具有对生成保密认证密钥所有必需的所有数据的访问权：
- [0316] ○读取器的保密主密钥，
- [0317] ○卡的证书，
- [0318] ○PIN 邮包挑战，
- [0319] ○PIN 邮包挑战上的卡密码。
- [0320] 使用生成的保密认证密钥，认证服务器可以用与它使传统强认证令牌生成的 OTP 或者 MAC 生效的方式相同的方式使 OTP 或者 MAC 生效。
- [0321] 代替地，认证服务器可以将图 13 或者 14 中所示任一过程用于生效操作。
- [0322] 结合图 13 的过程，假设使用变换 A (1306) 和变换 B (1307) 这一序列来变换由读取器产生的密码。出于生效目的，服务器使 OTP 或者 MAC 经历反变换 B (1327) 以产生修改的 OTP 或者 MAC，然后使参考密码经历变换 A (1325) 以产生修改的参考密码。最后，服务器执

行修改的参考密码与修改的 OTP 或者 MAC 的比较。

[0323] 结合图 14 的过程,假设如图 14 中所示使用位选择 (1355)、并置 (1356) 和位串变换 (1357) 这一序列来变换由读取器产生的密码以产生 OTP 或者 MAC。出于生效目的,服务器使 OTP 或者 MAC 经历图 14 的位流和扩展处理 1359 和 1360 以产生修改的 OTP 或者 MAC。服务器使参考密码经历操作 1364 以产生修改的参考密码。最后,服务器执行修改的参考密码与修改的 OTP 或者 MAC 的比较 (1365) 以实现生效。

[0324] 前文已经描述包括方法或者设备的若干方面或者实施例。在另一方面中,本发明包括在计算机可读介质上记录的指令序列,这些指令在由处理器执行时实现如已经描述的那样的方法。也可以通过数字网络如因特网来实现软件交付。因而在又一方面中本发明涵盖包括指令序列的信息承载信号,这些指令在由处理器执行时实现如已经描述的那样的方法。

[0325] 尽管已经用一些细节描述了本发明的若干实施例,但是应当理解这一描述为举例而不是限制;本发明的范围将由所附权利要求确定。

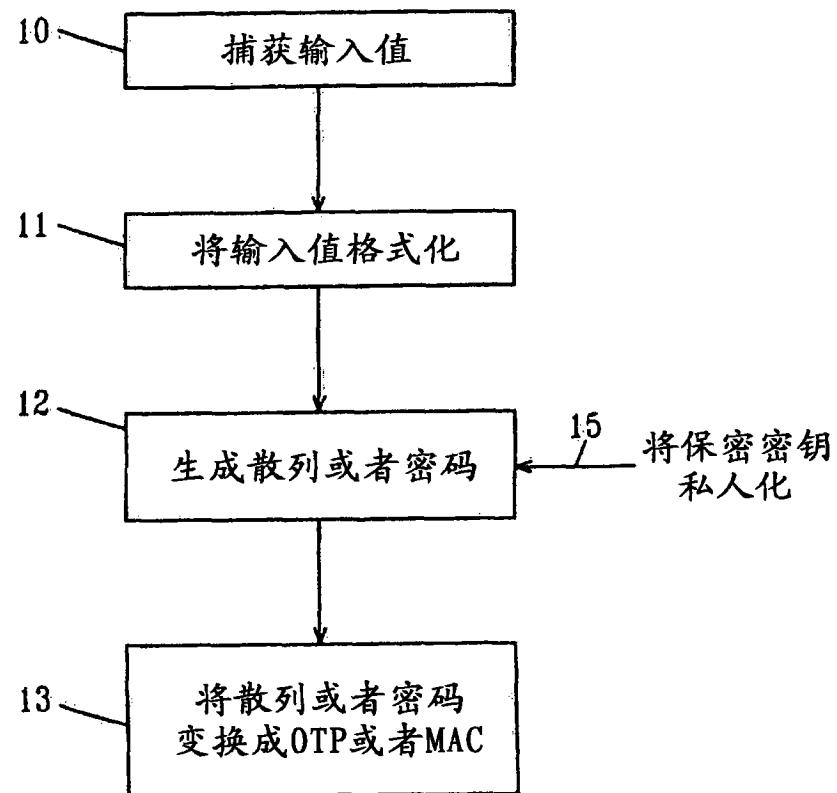


图 1

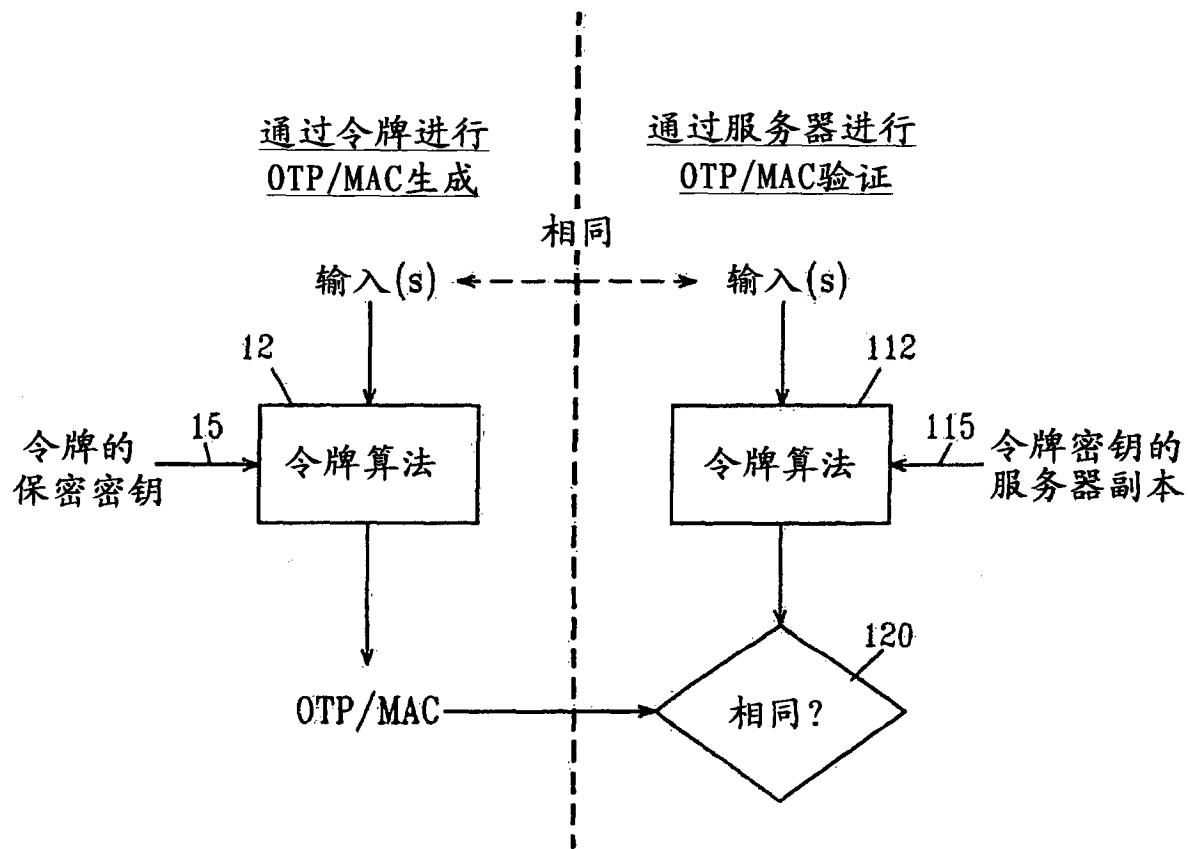


图 2

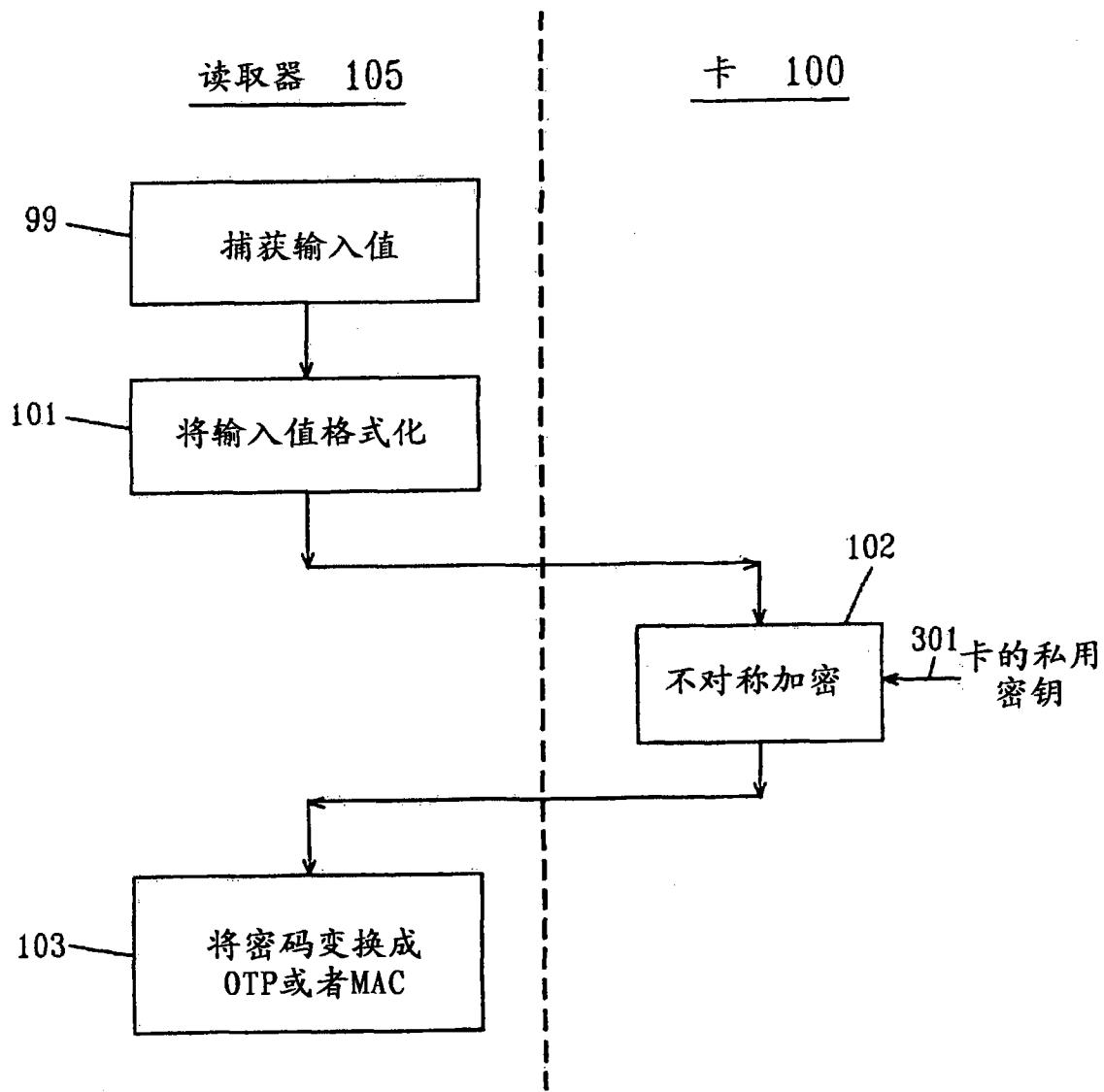


图 3

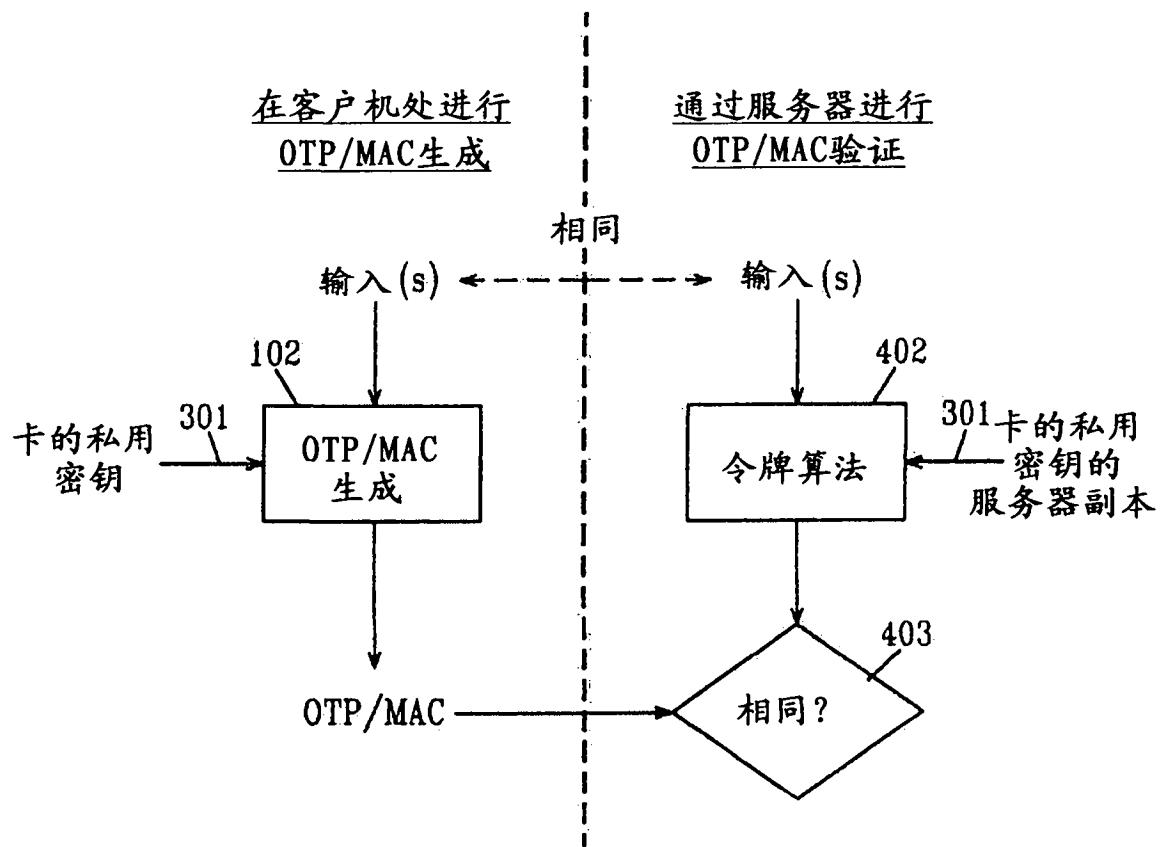


图 4

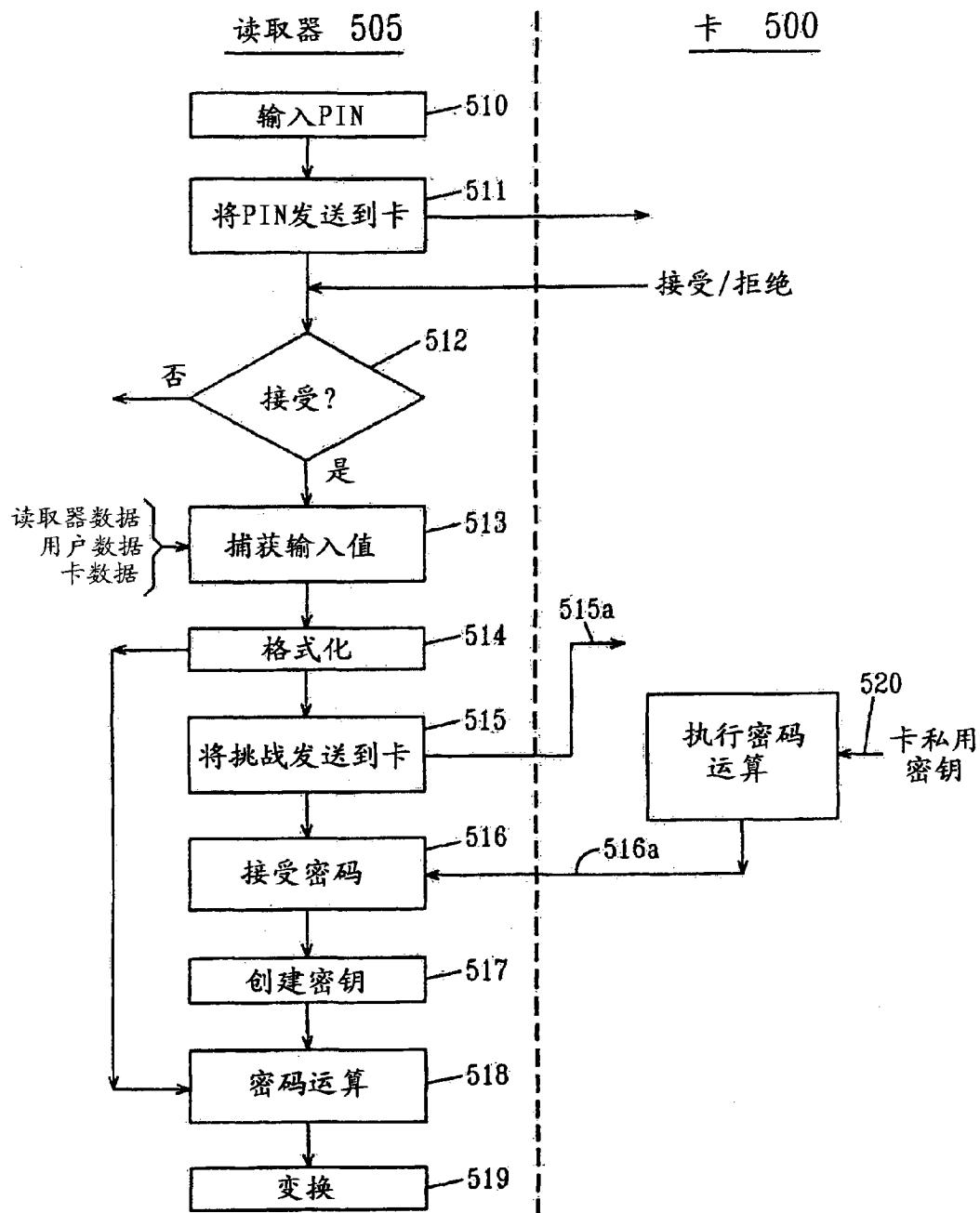


图 5

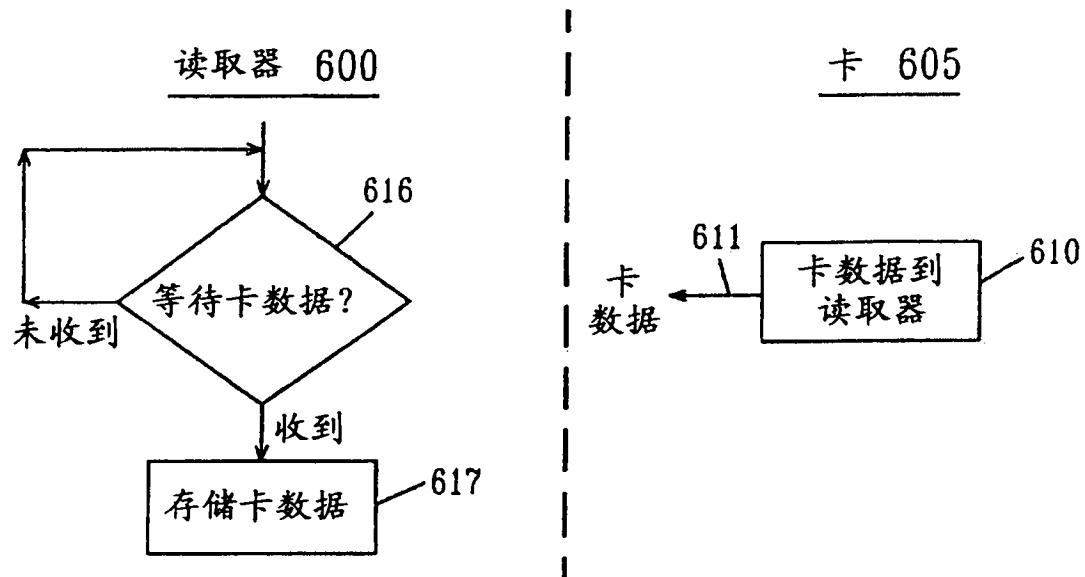


图 6

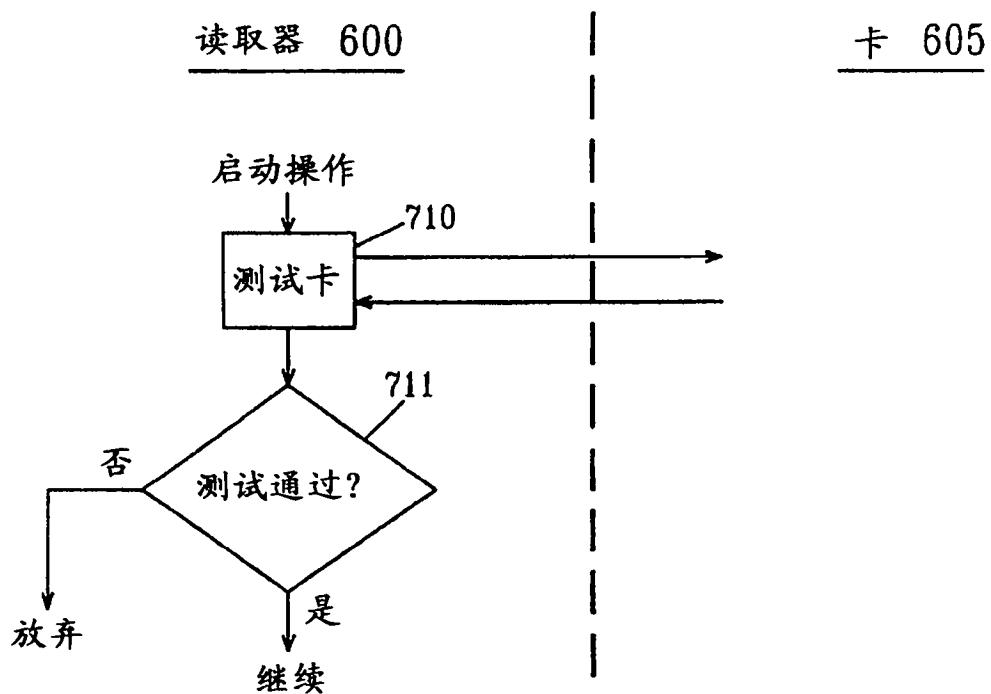


图 7

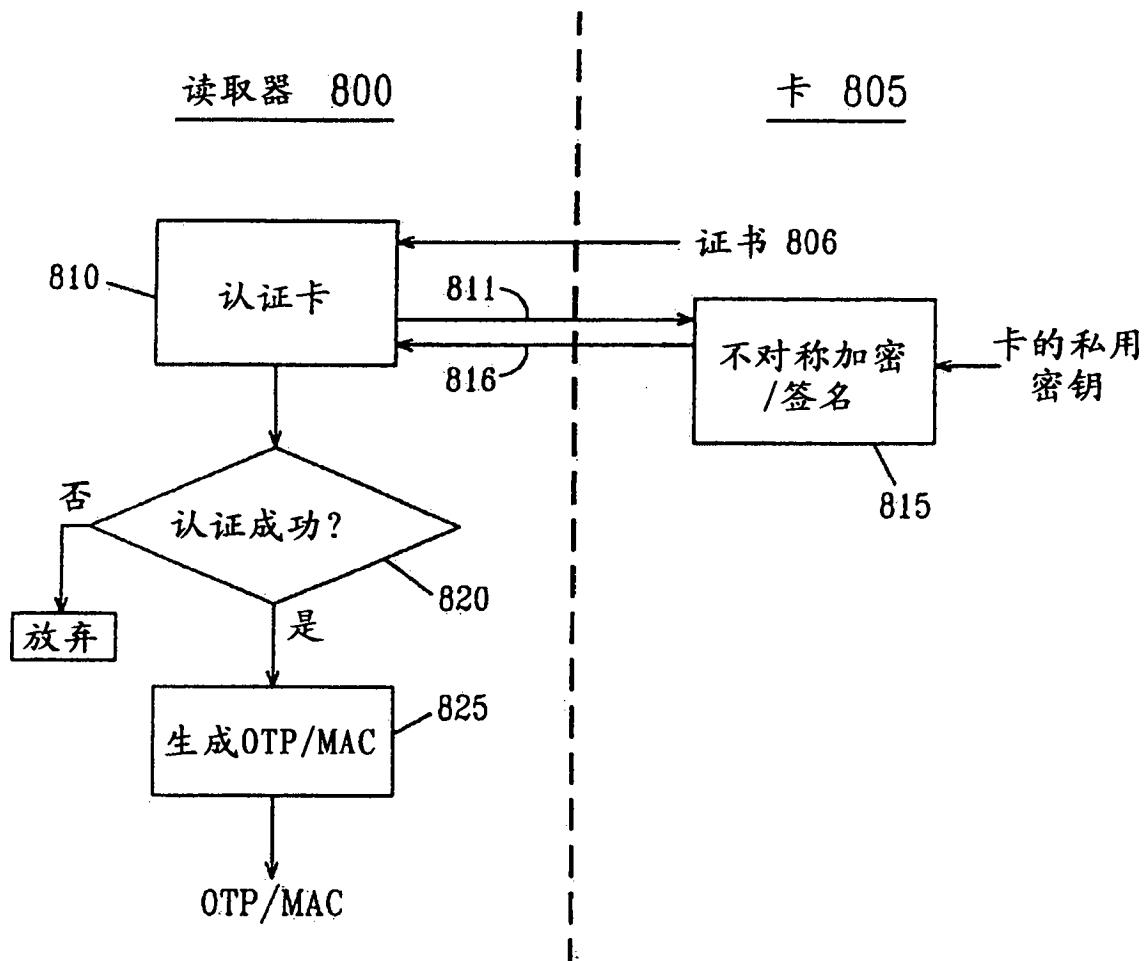


图 8

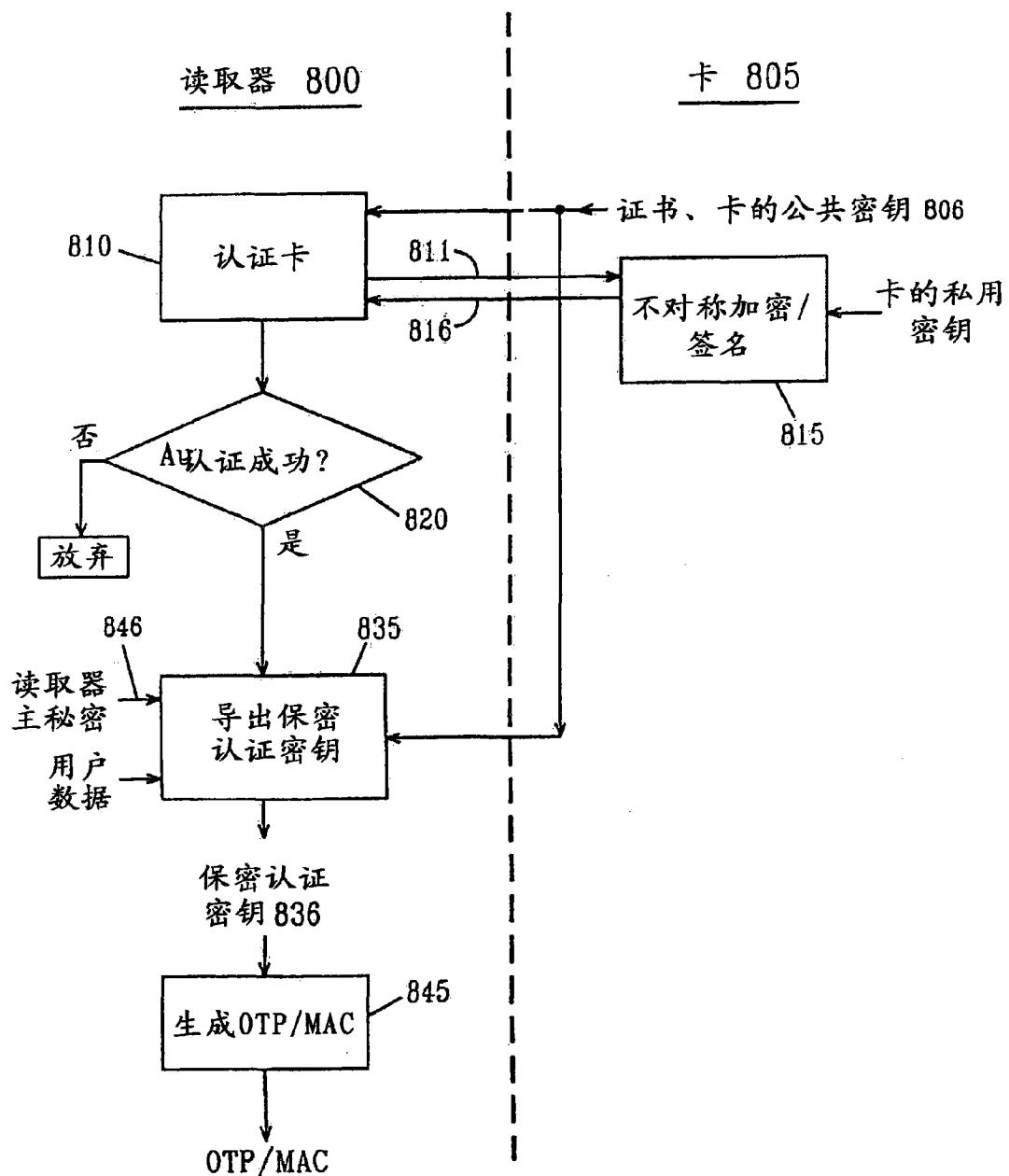


图 9

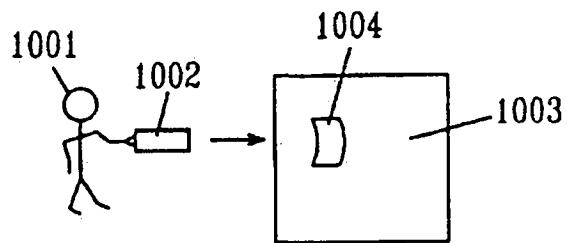


图 10

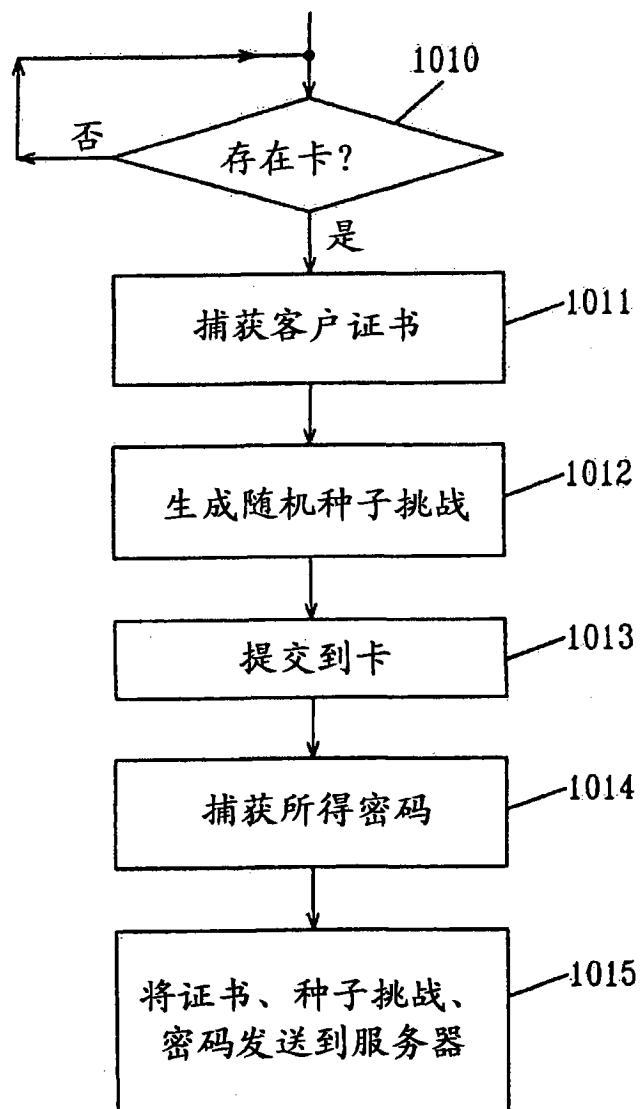


图 11

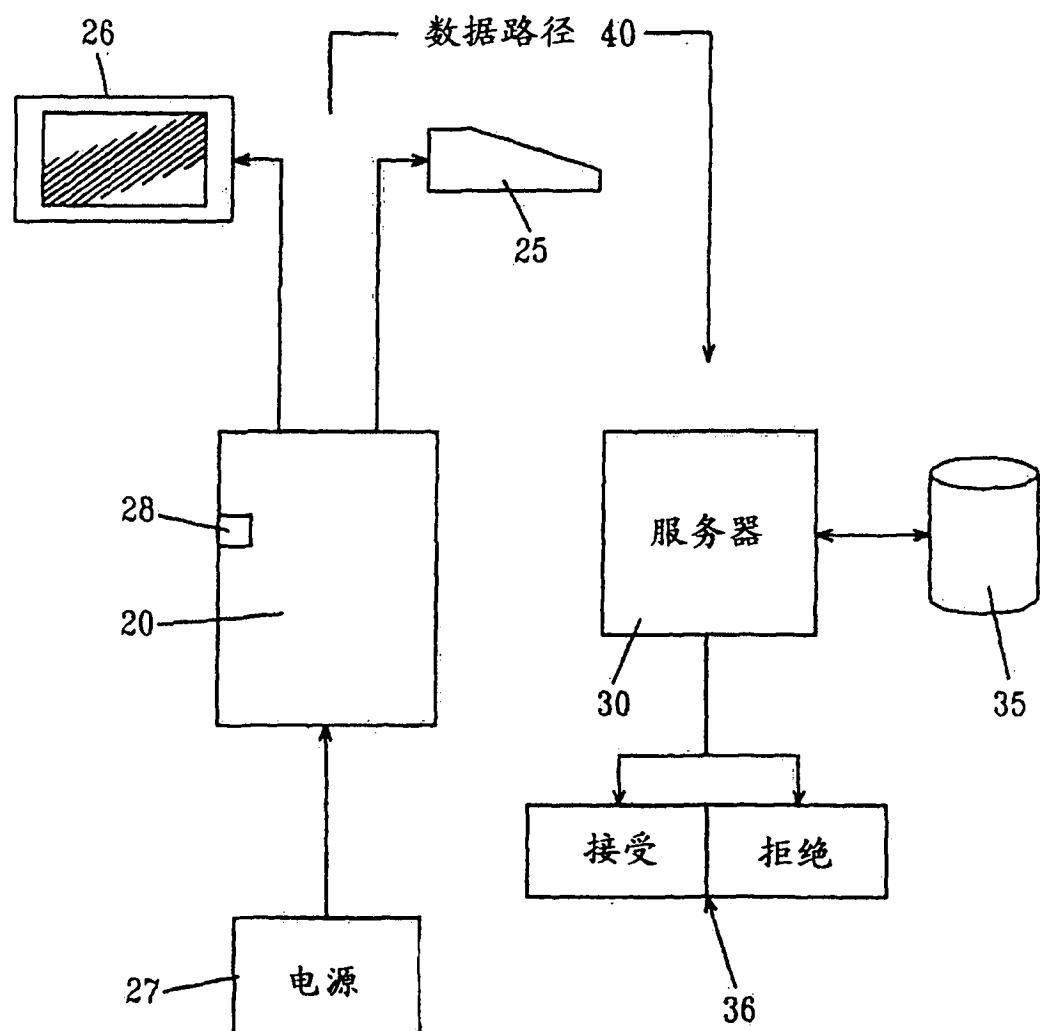


图 12

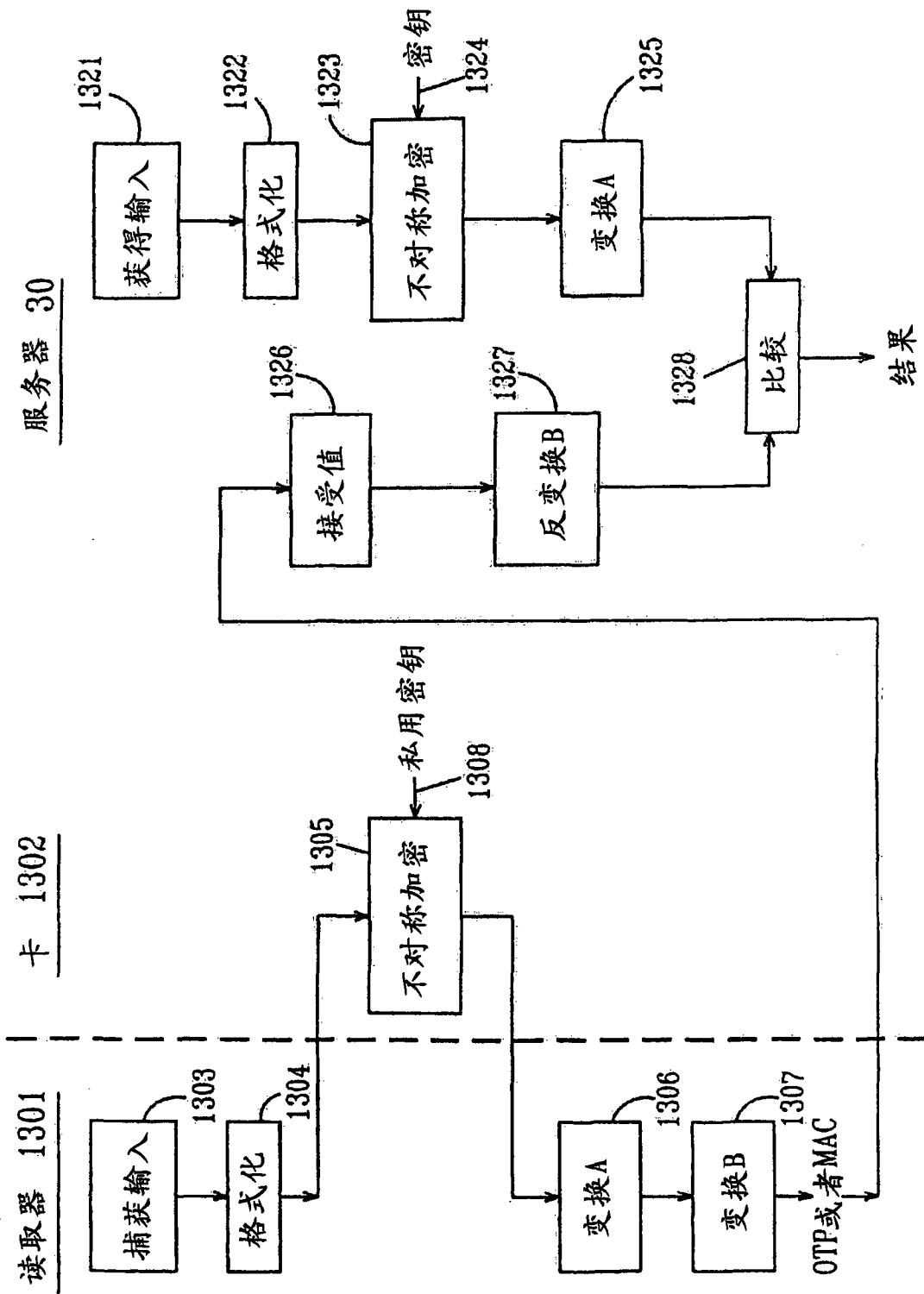


图 13

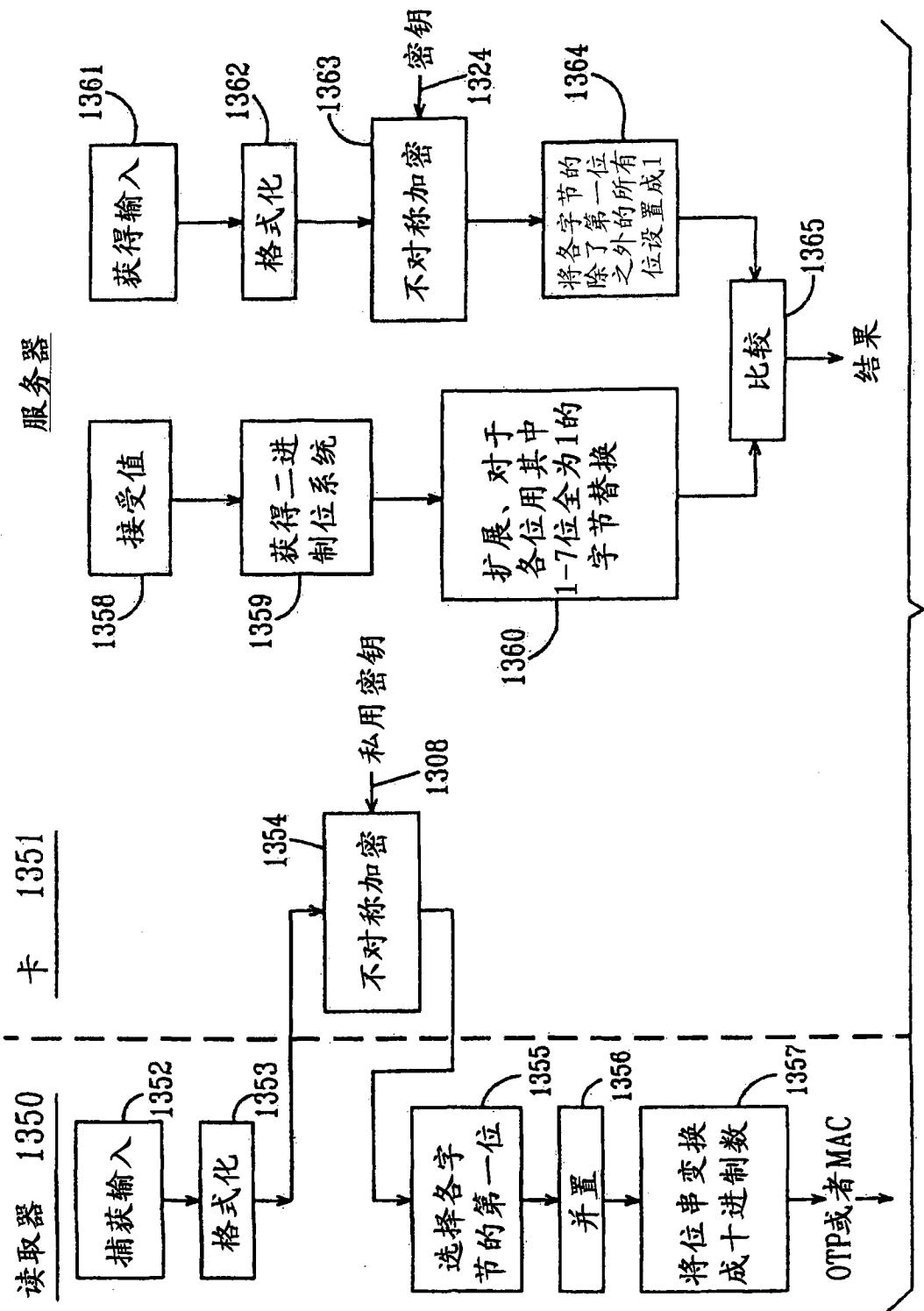


图 14